



STIC EIC 2100 Search Request Form

116994
(86)

Today's Date:

March 16, 2004

What date would you like to use to limit the search?

Priority Date: 1/8/98 Other:

Name : Michael Simitoski

AU : 2134 Examiner # : ~~70018~~ 79943

Room # : 5R03 Phone : 305-8191

Serial # : 09/764,794

Format for Search Results (Circle One):

PAPER DISK EMAIL

Where have you searched so far?

USP DWPI EPO JPO ACM IBM TDB

IEEE INSPEC SPI Other

Is this a "Fast & Focused" Search Request? (Circle One) YES NO

A "Fast & Focused" Search is completed in 2-3 hours (maximum). The search must be on a very specific topic and meet certain criteria. The criteria are posted in EIC2100 and on the EIC2100 NPL Web Page at <http://ptoweb/patents/stic/stic-tc2100.htm>.

What is the topic, novelty, motivation, utility, or other specific details defining the desired focus of this search? Please include the concepts, synonyms, keywords, acronyms, definitions, strategies, and anything else that helps to describe the topic. Please attach a copy of the abstract, background, brief summary, pertinent claims and any citations of relevant art you have found.

I need to find art on two main limitations: (1) why you'd want to encrypt a message, data, etc. with a key derived *partially (based on other things also)* from the data specific to/dependent on the message (like a hash, crc, signature, the message itself, part of the message). The most obvious reason is to make the key message specific to prevent replay attacks (where someone who intercepted the key wouldn't be able to use the same key again on another message) and (2) when sending the message, appending (in plaintext) the data specific to/dependent on the message to the encrypted message to be read by the recipient.

STIC Searcher Geoffrey St. Leger Phone 308-7800

Date picked up 3/16/4 Date Completed 3/16/4



L Number	Hits	Search Text	DB	Time stamp
-	27	@ad<19980107 and (message adj specific adj data)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 10:46
-	13	@ad<19980107 and encrypt\$3 same (message adj specific)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 10:46
-	5	((("5,930,399") or ("6,108,784") or ("6,311,058") or ("6,496,928") or ("6,356,956"))).PN.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 12:51
-	22	(message) same (signature) same ("second key")	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 13:40
-	496	@ad<19980107 AND (checksum same transmission same error)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 13:40
-	79	@ad<19980107 AND (checksum same transmission same error) and mobile	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 13:40
-	30	((@ad<19980107 AND (checksum same transmission same error) and mobile) and encrypt\$3	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 13:43
-	2413	ip and header and checksum	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 13:47
-	48	(ip and header and checksum) and @ad<19980107 and mobile	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 13:47
-	19	((ip and header and checksum) and @ad<19980107 and mobile) and phone	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 13:46
-	1401	ip and (header same checksum)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 13:49
-	27	(ip and (header same checksum)) and @ad<19980107 and mobile	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 13:47
-	9	((ip and (header same checksum)) and @ad<19980107 and mobile) and phone	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 13:47
-	159	ip same header same checksum same message	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 13:49
-	22	@ad<19980107 and (ip same header same checksum same message)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 13:50
-	1	@ad<19980107 and (ip same header same (checksum near3 error) same message)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 13:55
-	1	("20020046343").PN.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 14:21

title
scan md

-	1	((("20020046343").PN.) and bias\$3	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 14:25
-	87	@ad<19980107 and (bias\$3 same key same deriv\$5)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 14:26
-	0	@ad<19980107 and (bias\$3 same key same deriv\$5 same ("MAC" HMAC hash))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 14:26
-	8	@ad<19980107 and (bias\$3 same key same deriv\$5) and ("MAC" HMAC hash)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 14:29
-	46	@ad<19980107 and (hash) same (key near deriv\$5)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 14:30
-	0	@ad<19980107 and ((hash) same (key near deriv\$5) same bias\$3)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 14:30
-	0	@ad<19980107 and ((hash) same (key near deriv\$5) same (bias\$3 seed\$3))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 14:30
-	0	@ad<19980107 and ((hash) same (key near2 deriv\$5) same (bias\$3 seed\$3))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 14:30
-	42	@ad<19980107 and ((key near2 deriv\$5) same (bias\$3 seed\$3))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 14:32
-	1	@ad<19980107 and ((hash mac hmac digest) same (key near2 deriv\$5) same (bias\$3 seed\$3))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 14:35
-	93	@ad<19980107 and ((hash mac hmac digest) same (key near2 deriv\$5))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 14:49
-	82	@ad<19980107 and ((hash digest) same (key near2 deriv\$5))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 14:56
-	42	@ad<19980107 and ((bias\$3 seed\$3) same (key near2 deriv\$5))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 15:01
-	0	@ad<19980107 and (((hash digest) near seed) same (key near deriv\$5))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 15:01
-	0	@ad<19980107 and (((hash digest) near3 seed) same (key near2 deriv\$5))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 15:02
-	0	@ad<19980107 and (((hash digest) near3 seed) near5 (key near2 deriv\$5))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 15:02
-	40	@ad<19980107 and ((hash digest) near3 (seed\$3 bias\$3))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 15:21
-	1	6079018.pn. and hash\$3	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/03/15 15:22

file
scanned

file
scanned

-	0	6079018.pn. and hash\$3 same deriv\$5	USPAT; US-PGPUB; EPO; JPO; IBM TDB	2004/03/15 15:22
-	1	6079018.pn. and hash\$3 same key	USPAT; US-PGPUB; EPO; JPO; IBM TDB	2004/03/15 15:24
-	1	6079018.pn. and hash\$3 same (key near2 generat\$3)	USPAT; US-PGPUB; EPO; JPO; IBM TDB	2004/03/15 15:24

Set	Items	Description
S1	5735247	MESSAGE? ? OR EMAIL OR MAIL OR TEXT OR DATA OR INFORMATION OR CODE? ? OR VALUE? ? OR NUMBER? ? OR BYTE? ? OR BIT? ? OR WORD? ? OR PACKET? ? OR FRAME? ? OR DATAGRAM? ?
S2	/ 14078	KEY? ?(7N)(BASE? ? OR BASING OR DEPENDENT OR DEPENDENCE OR RELIAN?? OR CONTINGENT OR HASH??? OR FUNCTION OR DERIV???) (7N-S1)
S3	1541731	S1(5N)(SEND??? OR SENT OR TRANSMIT? OR TRANSFER???? OR TRANSMISSION OR FORWARD??? OR RELAY??? OR CONVEY? OR PROVID? OR PROVISION? OR DELIVER??? OR COMMUNICAT? OR EXCHANG? OR BROADCAST??? OR DISTRIBUT??? OR RECEIV? OR OBTAIN?)
S4	24554	CIPHER? OR CYPHER? OR ENCRYPT? OR ENCIPHER? OR ENCRYPT? OR DECRYPT? OR DECIPHER? OR DECRYPT? OR UNENCIPHER? OR UNENCRYPT? OR UNCIPHER?
S5	1510	S2 AND S3 AND S4
S6	10204	KEY? ?(5N)(DEPENDENT OR DEPENDENCE OR RELIAN?? OR CONTINGENT OR FUNCTION OR DERIV???)
S7	3380	S6(7N)S1
S8	246	S7 AND S3 AND S4
S9	246	KEY? ?(7N)S4
S10	217	S8 AND S9
S11	3136267	MESSAGE? ? OR EMAIL OR MAIL OR TEXT OR DATA OR INFORMATION OR CODE? ?
S12	2422	S6(7N)S11
S13	168	S10 AND S12
S14	886155	MESSAGE? ? OR EMAIL OR MAIL OR TEXT OR CODE? ?
S15	799	S6(7N)S14
S16	63	S13 AND S15
S17	1064443	S1(5N)(SEND??? OR SENT OR TRANSMIT? OR TRANSFER???? OR TRANSMISSION OR FORWARD??? OR RELAY??? OR CONVEY? OR DELIVER??? OR COMMUNICAT? OR EXCHANG? OR BROADCAST??? OR DISTRIBUT??? OR RECEIV?)
S18	17126	KEY(3N)(ESTABLISH? OR GENERAT? OR CREAT???? OR FASHION? OR CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR PRODUC???? OR DEVELOP? OR BUILT OR BUILD?)
S19	4865	KEY(5N)(COMPUTE OR COMPUTES OR COMPUTED OR COMPUTING OR DETERMIN? OR DISCERN? OR DERIV? OR CALCULA?)
S20	138	S10 AND S17 AND S18:S19
S21	95	S20 NOT S16
S22	61	S12 AND S21
S23	1236	SHARED() (KEY OR DATA OR INFORMATION OR VALUE? ? OR NUMBER? ? OR CODE? ?)
S24	10	S5 AND S23

STIC Search Results

Message encrypted with key derived in
part ~~the~~ the message. (1/2)
(From)

16/5/4 (Item 4 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

05482515 **Image available**
TRANSACTION INFORMATION PROCESSING METHOD, TRANSACTION INFORMATION
PROCESSOR, AND INFORMATION RECORDING MEDIUM

PUB. NO.: 09-097315 [JP 9097315 A]
PUBLISHED: April 08, 1997 (19970408)
INVENTOR(S): MATSUMURA SHUICHI
TAKAHASHI MASASHI
YURA AKIYUKI
APPLICANT(s): TOPPAN PRINTING CO LTD [000319] (A Japanese Company or
Corporation), JP (Japan)
APPL. NO.: 07-253277 [JP 95253277]
FILED: September 29, 1995 (19950929)
INTL CLASS: [6] G06K-017/00; B42D-015/10; G06K-019/073; G09C-001/00;
G09C-001/00; H04L-009/32
JAPIO CLASS: 45.3 (INFORMATION PROCESSING -- Input Output Units); 30.1
(MISCELLANEOUS GOODS -- Office Supplies); 44.3 (COMMUNICATION
-- Telegraphy); 44.9 (COMMUNICATION -- Other)

ABSTRACT

PROBLEM TO BE SOLVED: To **provide** a transaction **information** processor
which can surely detect an illegal use and data alteration and has an
extremely high security.

SOLUTION: An external processor 200 reads a card ID code and stored data
(transaction relative data) out of the **information** recording medium 100.
A diversifying **function** part 302 generates a diversification **key**
according to the card ID **code** and a count value and a **cipher key**
constituting the stored data and a **ciphering** function part 303 generates
adequacy information according to the diversification **key** and **ciphering**
key and compares the information with adequacy information read out of
the **information** recording medium 100 to judge the adequacy of the
information recording medium 100. When a transaction is made, transaction
relative data and adequacy information are generated with the transaction
data and a new automatically counted value and written in the **information**
recording medium 100.

16/5/5 (Item 5 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

05429554 **Image available**
ELECTRONIC APPARATUS AND ITS OPERATION CONTROL METHOD

PUB. NO.: 09-044354 [JP 9044354 A]
PUBLISHED: February 14, 1997 (19970214)
INVENTOR(s): KAWAMURA HARUMI
APPLICANT(s): SONY CORP [000218] (A Japanese Company or Corporation), JP
(Japan)
APPL. NO.: 07-212633 [JP 95212633]
FILED: July 28, 1995 (19950728)
INTL CLASS: [6] G06F-009/06; G06F-001/00; G06F-013/00; G09C-001/00;
H04L-009/32; H04N-007/167
JAPIO CLASS: 45.1 (INFORMATION PROCESSING -- Arithmetic Sequence Units);
44.3 (COMMUNICATION -- Telegraphy); 44.6 (COMMUNICATION --
Television); 44.9 (COMMUNICATION -- Other); 45.2 (INFORMATION
PROCESSING -- Memory Units); 45.9 (INFORMATION PROCESSING --
Other)
KEYWORD: R131 (INFORMATION PROCESSING -- Microcomputers &
Microprocessors)

ABSTRACT

PROBLEM TO BE SOLVED: To enable other companies to use each independently

developed application by transmitting a control signal, which includes preliminarily determined **cipher** information and has a prescribed format, an apparatus on the control side and setting the application to the executable state by an apparatus on the controlled side in the case of reception of the control signal including preliminarily determined **cipher** information.

SOLUTION: When receiving a target key code from a target (2), a controller multiplies a **cipher** function by this target key code to calculate an application key code. An open command of the application to which the application number and the calculated application key code are added is transmitted to the target (3). The target confirms whether the decoded result is equal to its own target key code or not; and if it is equal, the target validates the open command of the application K and enters into the open state that the application can be executed.

16/5/6 (Item 6 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

05359599 **Image available**
INFORMATION RECORDING MEDIUM

PUB. NO.: 08-315099 [JP 8315099 A]
PUBLISHED: November 29, 1996 (19961129)
INVENTOR(s): MATSUMURA SHUICHI
TAKAHASHI MASASHI
APPLICANT(s): TOPPAN PRINTING CO LTD [000319] (A Japanese Company or Corporation), JP (Japan)
PUB. NO.: 07-118799 [JP 95118799]
FILED: May 17, 1995 (19950517)
INTL CLASS: [6] G06K-019/073; G06F-012/14; G06F-017/60; G06F-019/00; G09C-001/00; H04L-009/00; H04L-009/10; H04L-009/12
JAPIO CLASS: 45.3 (INFORMATION PROCESSING -- Input Output Units); 44.3 (COMMUNICATION -- Telegraphy); 44.9 (COMMUNICATION -- Other); 45.2 (INFORMATION PROCESSING -- Memory Units); 45.4 (INFORMATION PROCESSING -- Computer Applications)

ABSTRACT

PURPOSE: To provide an information recording medium capable of surely detecting illegal use or data alteration and having extremely high security.

CONSTITUTION: An external processor 2 reads out the ID code P1 of an information recording medium 1, a transaction count value P2 and stored data P. Diversification function part 23 prepares a diversification key K' based upon the ID code P1, the count value P2 and a cipher key K and a ciphering function part 24 prepares validity information based upon the key K' and the stored data P and compares the prepared information with validity information read out from the medium 1. When the medium 1 is valid and illegal action is not executed, the contents of both the information coincide with each other, so that the existence of illegality or alteration can be surely judged.

16/5/7 (Item 7 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

04458922 **Image available**
FILE SECURITY SYSTEM

PUB. NO.: 06-102822 [JP 6102822 A]
PUBLISHED: April 15, 1994 (19940415)
INVENTOR(s): HIRATA KOZO
APPLICANT(s): ROORERU INTELLIGENT SYST KK [000000] (A Japanese Company or Corporation), JP (Japan)

APPL. NO.: 03-273501 [91273501]
FILED: September 26, 1991 (19910926)
INTL CLASS: [5] G09C-001/00; G06F-012/00; G06F-012/14
JAPIO CLASS: 44.9 (COMMUNICATION -- Other); 45.2 (INFORMATION PROCESSING
-- Memory Units)
JAPIO KEYWORD: R138 (APPLIED ELECTRONICS -- Vertical Magnetic &
Photomagnetic Recording)
JOURNAL: Section: P, Section No. 1770, Vol. 18, No. 376, Pg. 51, July
14, 1994 (19940714)

ABSTRACT

PURPOSE: To ensure security of information by **cyphering** secret information by **data** cryptographic **key** and recording and **transferring** the **data** cryptographic **key** **cyphered** by means of cryptographic **key** means.

CONSTITUTION: A terminal security unit 15 as a kind of **cyphering** devices takes a form of a black box and a proper cryptographic key TK whose contents are automatically extinguished when unsealing is done e.g. by illegal reverse engineering and acquired only by a user is sealed. The cryptographic **key** TK itself has not a **function** for directly **cyphering** plain text information (X), plays a role of a kind of master **keys**, **cyphers** a **data** cryptographic **key** DEX and is **provided** with the **function** of further **cyphering** the '**key**' on algorithm for **cyphering** processing of the plain text information. The data cryptographic **key** means itself is **cyphered** and freely stored or transferred.

16/5/8 (Item 8 from file: 347)
DIALOG(R) File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

04352416 **Image available**
SATELLITE DATA BROADCASTING SYSTEM

PUB. NO.: 05-344116 [JP 5344116 A]
PUBLISHED: December 24, 1993 (19931224)
INVENTOR(s): UENO NOBUO
APPLICANT(s): FUJITSU LTD [000522] (A Japanese Company or Corporation), JP
(Japan)
APPL. NO.: 04-151032 [JP 92151032]
FILED: June 11, 1992 (19920611)
INTL CLASS: [5] H04L-009/06; H04L-009/14; H04B-007/212; H04L-012/18
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 34.4 (SPACE DEVELOPMENT
-- Communication); 44.2 (COMMUNICATION -- Transmission
Systems)
JOURNAL: Section: E, Section No. 1530, Vol. 18, No. 174, Pg. 145,
March 24, 1994 (19940324)

ABSTRACT

PURPOSE: To detect the noncoincidence of keys at a **receiving** station without decreasing the **packet** **transmission** capacity of **transmitting** information concerning the satellite data **broadcasting** system for **cyphering** and **transmitting** the **transmitting** information.

CONSTITUTION: In the satellite **data** **broadcasting** system **provided** with a center station A and a receiving station B, the center station is **provided** with a key version **number** generating means 4 to generate and **transmit** the **number** of versions for network keys, key information generating means 2 to generate **key** information by **cyphering** the network **keys** and adding the version **number** of **key**, and **key** edition number fetching **function** 31 added to a **frame** control **code** generating section 3. The **receiving** station is **provided** with a **key** **information** **receiving** means 6 to separate the key version number from the inputted information and to store it, and key version number collating means 7 to compare the **key** **information** **receiving** means with the respective key version number extracted at a **frame** control **code** extracting section 5 and to report the collated result.

16/5/9 (Item 9 from file: 347)
DIALOG(R) File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

0381214 **Image available**

PICTURE INFORMATION CIPHERING METHOD

PUB. NO.: 05-304614 [JP 5304614 A]
PUBLISHED: November 16, 1993 (19931116)
INVENTOR(s): TOMITA YASU HARU
SUZUKI MASAHIRO
APPLICANT(s): NEC CORP [000423] (A Japanese Company or Corporation), JP
(Japan)
NEC SHIZUOKA LTD [489142] (A Japanese Company or Corporation)
, JP (Japan)
APPL. NO.: 04-083790 [JP 9283790]
FILED: April 06, 1992 (19920406)
INTL CLASS: [5] H04N-001/44; H04L-009/06; H04L-009/14
JAPIO CLASS: 44.7 (COMMUNICATION -- Facsimile); 44.3 (COMMUNICATION --
Telegraphy)
JOURNAL: Section: E, Section No. 1512, Vol. 18, No. 105, Pg. 149,
February 21, 1994 (19940221)

ABSTRACT

PURPOSE: To hold a secrecy by providing a **function** which selects plural **keys**, and selecting a **code key** according to time information, in the **cipherment** system of a facsimile terminal equipment.

DESCRIPTION: Picture information read by a photoelectric converting part 1 is compressed by a compressing part 2, and transmitted to a **ciphering** part 3. The **ciphering** part 3 is constituted of a known data scramble circuit constituted of a shift register and an EX-OR circuit, and the **ciphering** part 3 operates the scramble of the inputted compressed picture information by writing a key as the initial value of the shift register. The **ciphered** compressed picture information is modulated by a modulating part 7, and transmitted from a network control part 8 to a line 9. A device control part 4 detects the time of a time part 19 set at a transmitter side, a password, and the time **information** of the other party, and **communicates** them to a key selecting part 5. The key selecting part 5 selects a matching/mismatching, operates a function arithmetic operation, and communicates the result to a key table 6.

16/5/10 (Item 10 from file: 347)
DIALOG(R) File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

03961342 **Image available**

MESSAGE VERIFICATION SYSTEM

PUB. NO.: 04-326442 [JP 4326442 A]
PUBLISHED: November 16, 1992 (19921116)
INVENTOR(s): TANAKA TAKESHI
IWASE FUMIYUKI
HIRANO KAZUYA
APPLICANT(s): N T T DATA TSUSHIN KK [000000] (A Japanese Company or
Corporation), JP (Japan)
APPL. NO.: 03-097012 [JP 9197012]
FILED: April 26, 1991 (19910426)
INTL CLASS: [5] G06F-013/00; G06F-015/00
JAPIO CLASS: 45.2 (INFORMATION PROCESSING -- Memory Units); 45.4
(INFORMATION PROCESSING -- Computer Applications)
JOURNAL: Section: P, Section No. 1513, Vol. 17, No. 163, Pg. 161,
March 30, 1993 (19930330)

ABSTRACT

PURPOSE: To obtain a technique which can certify the justification of a message which is received by an arbitrary person and can certify the justification of the transmission source of the received message in a communication network system which is utilized by unspecified and multiple registers through the use of an IC card having a ciphering function.

CONSTITUTION: At the time of transmitting the message, one's name is signed to the transmitted message by using individual keys peculiar to the IC cards 11 and 15, and a cipher function, and the message with an electric signature is transmitted to a communication opposite party with ID information. At the time of receiving the message, the individual key of the transmission source of the message is generated from a parameter for individual key generation and transmitted ID information, and the message with the signature is certified by using the individual key and the cipher function. Thus, the forgery and forge of the message and illegal impersonation by a third person can be prevented.

16/5/11 (Item 11 from file: 347)
DIALOG(R) File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

03-1438 **Image available**
JAP. INTL. MESSAGE COMMUNICATION SYSTEM

APP. NO.: 03-014338 [JP 3014338 A]
PUBLISHED: January 23, 1991 (19910123)
INVENTOR(s): TAKE RIICHIRO
APPLICANT(s): FUJITSU LTD [000522] (A Japanese Company or Corporation), JP
(Japan)
APPL. NO.: 01-150143 [JP 89150143]
FILED: June 13, 1989 (19890613)
INTL CLASS: [5] H04L-009/06; H04L-009/14
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy)
JOURNAL: Section: E, Section No. 1051, Vol. 15, No. 130, Pg. 97, March
29, 1991 (19910329)

ABSTRACT

PURPOSE: To attain communication processing on a required data while preventing message communication from being concentrated by using a received today's decoding key to decode a ciphered message based upon an already received ciphering key of the same date.

CONSTITUTION: A news board 10 having a disclosed key calendar 11 and a today's decoding key 12 transmits a ciphering key of a data specified by a ciphering key request to a requesting source at the time of receiving the request from the requesting source, or transmits a today's decoding key at the time of receiving a today's decoding key request from the requesting source. A work station 30 is provided with a message communication function means 31, which includes a ciphering function means 32 for ciphering a message to be transmitted by using the received ciphering key and a decoding function means 33 for decoding a message ciphered by the received ciphering key of the same date. Consequently, message communication on a network 20 can be prevented from being concentrated and a message can be transferred to a required destination on a required data.

16/5/12 (Item 12 from file: 347)
DIALOG(R) File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

02252656 **Image available**
TELEPHONE SET FOR ENCRYPTED IC CARD

APP. NO.: 62-169556 [JP 62169556 A]
PUBLISHED: July 25, 1987 (19870725)

INVENTOR(s): KAMEDA TORU
TOMIYAMA KATSUMI
YAMAMOTO MASATAKA
APPLICANT(s): MITSUBISHI ELECTRIC CORP [000601] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 61-011363 [JP 8611363]
FILED: January 22, 1986 (19860122)
INTL CLASS: [4] H04M-001/274; H04K-001/00; H04L-009/02; H04M-001/66
JAPIO CLASS: 44.4 (COMMUNICATION -- Telephone); 44.2 (COMMUNICATION -- Transmission Systems); 44.3 (COMMUNICATION -- Telegraphy)
JOURNAL: Section: E, Section No. 572, Vol. 12, No. 9, Pg. 92, January 12, 1988 (19880112)

ABSTRACT

PURPOSE: To secure a double high-grade **information** protecting **function** for both a **key code** and an **enciphered** algorithm by using an IC card as a memory device for dial numbers and **enciphering** the dial number together with the **key code** supplied for decoding through the dial digit buttons of the IC card telephone when the dial number is stored in the IC card.

CONSTITUTION: An IC 12 card is put into a reading device 15 and a key code is inputted by means of the dial digit buttons 4 of a telephone. A CPU 7 set at the inside of the device 15 collates the input key code with the key code registered on the card 12. Then a command signal is delivered only when coincidence is **obtained** between both key **codes**. When an automatic dial **transmission** button 5 is pushed, the CPU 7 sends a request signal to the card 12 to extract the dial number data corresponding to the pushed button 5 and reads an **enciphered** dial number out of an EEPROM chip 14 to send it to the CPU 7. This dial number is decoded and restored to the original dial **number**. Then this original **number** is **sent** automatically to a telephone circuit via a telephone main body circuit 9.

16/5/13 (Item 13 from file: 347)
JAPIO File 347: JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

01390388 **Image available**
TERMINAL EQUIPMENT OF CATV

PUB. NO.: 59-101988 [JP 59101988 A]
PUBLISHED: June 12, 1984 (19840612)
INVENTOR(s): KANAI TSUTOMU
APPLICANT(s): PIONEER ELECTRONIC CORP [000501] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 57-211686 [JP 82211686]
FILED: December 02, 1982 (19821202)
INTL CLASS: [3] H04N-007/16
JAPIO CLASS: 44.6 (COMMUNICATION -- Television)
JOURNAL: Section: E, Section No. 270, Vol. 08, No. 217, Pg. 135, October 04, 1984 (19841004)

ABSTRACT

PURPOSE: To reinforce a furtive glance and eavesdropping preventive **function** by **ciphering** a **key code** signal given to a scramble decoder in relation to an intrinsic address signal from an address unit.

CONSTITUTION: A scramble decoder which **receives** an **information** from the address unit through a converter 21 **sends** out a **data information** to a controller 23. In this case, an intrinsic address signal from an address unit and a **ciphered key code** from a PROM 24 are inputted to the controller 23. The controller 23 operates the key code which is compared with the supplied data information and is **ciphered**, and the intrinsic address, and supplies a normal key **code obtained** as its result to a scramble decoder 22. By executing the processing in this way, the furtive glance and eavesdropping function can be reinforced.

16/5/27 (Item 14 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

012637854 **Image available**
WPI Acc No: 1999-443958/199937
Related WPI Acc No: 2002-655071
XRPX Acc No: N99-331117

Point-of- distribution stored value card activator
Patent Assignee: VISA INT SERVICE ASSOC (VISA-N)
Inventor: DAVIS V M; ROTH J R; ROTH J T
Number of Countries: 084 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9933033	A2	19990701	WO 98US27073	A	19981218	199937 B
AU 9919324	A	19990712	AU 9919324	A	19981218	199950
EP 1040456	A2	20001004	EP 98964134	A	19981218	200050
			WO 98US27073	A	19981218	
US 6298336	B1	20011002	US 9768196	P	19971219	200160
			US 98216509	A	19981218	
AU 758710	B	20030327	AU 9919324	A	19981218	200330

Priority Applications (No Type Date): US 9768196 P 19971219; US 98216509 A 19981218

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

WO 9933033 A2 E 53 G07F-007/10

Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW

AU 9919324 A G07F-007/10 Based on patent WO 9933033

EP 1040456 A2 E G07F-007/10 Based on patent WO 9933033

Designated States (Regional): BE DE FR GB

US 6298336 B1 G06F-017/60 Provisional application US 9768196

AU 758710 B G07F-007/10 Previous Publ. patent AU 9919324

Based on patent WO 9933033

Abstract (Basic): WO 9933033 A2

NOVELTY - Activator comprises a card dispensing machine with cards which have a security code derived from an issuer key. A secure application module has the issuer key and an encryption module deriving the security code. An activation control counter limit is checked and when it reaches a limit activation of the card is aborted.

USE - Activator is for activating smart cards at the point of distribution.

ADVANTAGE - Activator prevents theft of cards, minimizes losses to an insurer if a card is stolen and reduces card security costs.

DESCRIPTION OF DRAWING(S) - The drawing shows a stored value card activation system.

pp: 53 DwgNo 1/14

Terms: POINT; DISTRIBUTE; STORAGE; VALUE; CARD; ACTIVATE

Derwent Class: T01; T04; T05

International Patent Class (Main): G06F-017/60; G07F-007/10

File Segment: EPI

16/5/29 (Item 16 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

012470763 **Image available**
WPI Acc No: 1999-276871/199923
Related WPI Acc No: 1996-466993; 1997-298643; 1999-276077
XRPX Acc No: N99-207586

Encryption key transfer method in data communication system - involves forwarding message including signature and specific exponentiated function from one correspondent to that of other which utilizes message to compute specific session key

Patent Assignee: CERTICOM CORP (CERT-N)

Inventor: MENEZES A J; QU M; VANSTONE S

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 5896455	A	19990420	US 95442833	A	19950517	199923 B
			US 9866609	A	19980424	

Priority Applications (No Type Date): US 9866609 A 19980424; US 95442833 A 19950517

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
US 5896455	A	6	H04L-009/08	CIP of application US 95442833
				CIP of patent US 5761305

Abstract (Basic): US 5896455 A

NOVELTY - A message including a signature (SA) and specific exponentiated function is forwarded from correspondent (10) to a correspondent (12). The correspondent (12) utilizes the signature to verify the value of exponentiated function in the message. A session key (K') is computed by the correspondent (12) by exponentiating the exponentiated function by a private key (b).
DETAILED DESCRIPTION - The correspondent (10) selects a random integer (x) and exponentiating a specific function. The correspondent (10) computes session key (K) from public key (PB) of correspondent (12). The correspondent (12) utilizes public key (PA) of the correspondent (10). The session key (K) is computed by exponentiating function of public key (PB) of correspondent (12) with the function signature (SA).

USE - In data communication system.

ADVANTAGE - The protocols are modified to improve bandwidth requirements and computational efficiency of key agreement.

DESCRIPTION OF DRAWING(S) - The figure represents schematic representation of data communication system. (10,12) Correspondent.

Dwg. 1/1

Key Terms: ENCRYPTION ; KEY; TRANSFER; METHOD; DATA; COMMUNICATE; SYSTEM ; FORWARDING; MESSAGE; SIGNATURE; SPECIFIC; FUNCTION; ONE; MESSAGE; COMPUTATION; SPECIFIC; SESSION; KEY

Derwent Class: W01

International Patent Class (Main): H04L-009/08

International Patent Class (Additional): H04L-009/30

File Segment: EPI

16/5/31 (Item 18 from file: 350)

MAILING(R)File 350:Derwent WPIX

© 2004 Thomson Derwent. All rts. reserv.

011962329 **Image available**

WPI Acc No: 1998-379239/199833

XRPX Acc No: N98-296537

Verifying cryptographic postage evidencing method using fixed key set - generating several random verifier master keys which consist of fixed number of keys and generating pointer by applying pseudorandom algorithm to data unique to transaction evidencing device

Patent Assignee: PITNEY BOWES INC (PITB)

Inventor: CORDERY R A; LEE D K; PAULY S J; PINTSOV L A; RYAN F W; WEIANT M A

Number of Countries: 026 Number of Patents: 005

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 071144	A2	19980722	EP 97121937	A	19971212	199833 B
EP 0722662	A	19980623	CA 2222662	A	19971126	199841
EP 5982896	A	19991109	US 96772739	A	19961223	199954
US 6058193	A	20000502	US 96772739	A	19961223	200029

US 99340592 A 19990628
20030812 CA 2222662 A 19971126 200360

Priority Applications (No Type Date): US 96772739 A 19961223; US 99340592 A 19990628

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

EP 854444 A2 E 12 G07B-017/00

Designated States (Regional): AL AT BE CH DE DK ES FI FR GB GR IE IT LI

LT LU LV MC MK NL PT RO SE SI

CA 2222662 A G07B-017/02

US 5982896 A H04L-009/00

US 6058193 A H04L-009/00 Cont of application US 96772739

CA 2222662 C E G07B-017/02

Abstract (Basic): EP 854444 A

The method involves generating several random verifier master keys (18) to obtain a set (100) of verifier master keys consisting of a fixed number of keys. A pointer is generated by applying a pseudorandom algorithm to data unique to a transaction evidencing device (12). Several verifier token keys (34) are calculated to obtain a verifier token key set corresponding to the set of verifier master keys.

The verifier token **key** set is **encrypted** with a privacy **key**. The verifier token **key** set and the privacy key are distributed to verifiers (60). Master keys are **distributed** to postal and vendor data centres. The token **keys** are a **function** of the verifier master **keys** and a **code** valid for a limited time. The code is function of a time dependent parameter. The pointer algorithm is an appropriate cryptographic algorithm.

ADVANTAGE - Improves security of digital meters by providing simplified means for posts to validate indicia in real time.

Dwg. 2/7

Title Terms: VERIFICATION; CRYPTOGRAPHIC; POSTAGE; METHOD; FIX; KEY; SET; GENERATE; RANDOM; VERIFICATION; MASTER; KEY; CONSIST; FIX; NUMBER; KEY; GENERATE; POINT; APPLY; ALGORITHM; DATA; UNIQUE; TRANSACTION; DEVICE

Derwent Class: T01; T05

International Patent Class (Main): G07B-017/00; G07B-017/02; H04L-009/00

International Patent Class (Additional): H04L-009/32

File Segment: EPI

16/5/32 (Item 19 from file: 350)

DIALOG(R) File 350: Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

011930924 **Image available**

WPI Acc No: 1998-347834/199830

XPX Acc No: N98-271524

Encrypting data communication **method e.g. for distributed computer system - involves** encrypting data message **with encryption function using transmission encryption key to produce ciphertext** message

Patent Assignee: DIGITAL EQUIP CORP (DIGI)

Inventor: SPRATTE M

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
5764766	A	19980609	US 96661425	A	19960611	199830 B

Priority Applications (No Type Date): US 96661425 A 19960611

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

US 5764766 A 6 H04K-001/00

Abstract (Basic): US 5764766 A

The method involves generating a salt at a **data transmitting** system. The salt is then combined with a primary **encryption key** known at the **data transmitting** system and a **data receiving**

system. The primary **encryption key** and the salt are hashed to produce a transmitting **encryption key**.

A data message with an **encryption** function is **encrypted** using the transmitting **encryption key** to produce a **ciphertext** message. The salt and the **ciphertext message** are then **transmitted** to the **data receiving** system.

ADVANTAGE - Prevents timing problems. Avoids use of large **encryption keys**.

Dwg.2/2

Title Terms: DATA; COMMUNICATE; METHOD; DISTRIBUTE; COMPUTER; SYSTEM; DATA; MESSAGE; **ENCRYPTION** ; FUNCTION; TRANSMISSION; **ENCRYPTION** ; KEY; PRODUCE ; MESSAGE

Derwent Class: T01; W01; W02

International Patent Class (Main): H04K-001/00

File Segment: EPI

16/5/35 (Item 22 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

011826227 **Image available**

WPI App No: 1998-243137/199822

WPI App No: N98-192460

Public key encryption based method for digital signatures - involves combining values derived by hashing messages and derived from public keys to form multiple user digital signatures

Patent Assignee: HITACHI LTD (HITA)

Inventor: KURUMATANI H; TAKARAGI K

Number of Countries: 025 Number of Patents: 003

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 840478	A2	19980506	EP 97118704	A	19971028	199822 B
JP 10133576	A	19980522	JP 96290525	A	19961031	199831
US 6341349	B1	20020122	US 97961557	A	19971030	200208

Priority Applications (No Type Date): JP 96290525 A 19961031

Filed Patents: No-SR.Pub

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

EP 840478 A2 E 31 H04L-009/32

Designated States (Regional): AL AT BE CH DE DK ES FI FR GB GR IE IT LI

LT LU LV MC NL PT RO SE SI

JP 10133576 A 17 G09C-001/00

US 6341349 B1 G06F-001/24

Abstract (Basic): EP 840478 A

The digital signature method is used on a network (101) of computers. A first user (A) generates a message (110) that is passed to a second user (B) for comment (114) before passing to a final user (C). The message has a digital signature for the first user formed using a hashing system to find a first value. A number is obtained by translating a random number and its hash value found. The values are combined as the digital signature.

To verify the signature, the hash value of the message is formed. A number is obtained via a public key (Q) using a base point (P). The hash of this is compared with the signature.

ADVANTAGE - Provides a digital signature method that has high security and uses a short bit length for the signature.

Dwg.1/9

Title Terms: PUBLIC; KEY; **ENCRYPTION** ; BASED; METHOD; DIGITAL; SIGNATURE; COMBINATION; VALUE; DERIVATIVE; HASH; MESSAGE; DERIVATIVE; PUBLIC; KEY; FORM; MULTIPLE; USER; DIGITAL; SIGNATURE

Derwent Class: P85; T01; W01

International Patent Class (Main): G06F-001/24; G09C-001/00; H04L-009/32

File Segment: EPI; EngPI

16/5/38 (Item 25 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

Image available
WPI Acc No: 1997-451677/199742
XRPX Acc No: N99-190118

Manufacturer independent, authenticity identification device obtaining
method for service provider - involves storing code, from service
provider, obtained by RSA function having secret encryption key,
in write-once type area of card
Patent Assignee: ALFI SRL (ALFI-N); NOVARA TEC SYS AUTOMAZIONE SRL (NOVA-N)
Inventor: COLOMBO G; FORTINA E; IPPOLITO G; FORTINA M G E
Number of Countries: 003 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
IT 1269422	B	19970401	IT 94MI22	A	19940111	199742 B
US 5878137	A	19990302	US 95368937	A	19950105	199916
			US 97888197	A	19970703	
CH 689758	A5	19991015	CH 9531	A	19950106	199947

Priority Applications (No Type Date): IT 94MI22 A 19940111

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
US 5878137	A	5	H04K-001/00	Cont of application US 95368937
IT 1269422	B		G09F-000/00	
CH 689758	A5		B42D-015/10	

Title Terms: MANUFACTURE; INDEPENDENT; AUTHENTICITY; IDENTIFY; DEVICE;
OBTAIN; METHOD; SERVICE; STORAGE; CODE; SERVICE; OBTAIN; FUNCTION; SECRET
; ENCRYPTION ; KEY; WRITING; TYPE; AREA; CARD

IPC Class: P76; P85; T01; T04; W01; W02; W06

International Patent Class (Main): B42D-015/10; G09F-000/00; H04K-001/00

International Patent Class (Additional): G06K-003/00; G06K-019/06;

H04L-009/00

File Segment: EPI; EngPI

16/5/40 (Item 27 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

011033680 **Image available**
WPI Acc No: 1997-011604/199701
XRPX Acc No: N97-010181

Secure information communication method eg. for GPS system -
transmitting pseudorange correction signal at consecutive sequence of
times, and encrypting message using key which is function of
preceding correction value

Patent Assignee: TRIMBLE NAVIGATION LTD (TRIM-N)

Inventor: MELTON W C; SCHIPPER J F

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 5577122	A	19961119	US 94367440	A	19941229	199701 B

Priority Applications (No Type Date): US 94367440 A 19941229

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
US 5577122	A	34	H04K-001/00	

Abstract (Basic): US 5577122 A

The communication method comprises the steps of providing an LDS
reference station, having location coordinates that are known with high
accuracy, the reference station having an LDS signal antenna and
associated LDS signal receiver/processor for receiving and processing
location determination signals, or 'LD signals', from several LD
signal sources to determine spatial location and clock coordinates for
that station. An LDS mobile station is provided having an LDS signal

antenna and associated LD signal receiver/processor for receiving and processing LD signals from several LD signal sources to determine spatial location and clock coordinates for that station.

Each reference station and mobile station are caused to receive LD signals from several LD signal sources, numbered $j=1, 2, \dots, M$ (M greater than or equal to 2), with M greater than or equal to 2, in common view with each other, and to determine the LD signal values $LD(t;i;j)$ as a function of time t for that station, numbered i =reference and i =mobile, from the signals received from the M common view LD signal sources. The reference station determines location determination adjustment signal values, or 'LDA signal values', $LDA(t;ref;j)$ at one or more times t that, when added to the LD signal values $LD(t;ref;j)$ available at the reference station for the time t , produce spatial location coordinates that approximately agree with the known spatial location coordinates for the reference station for the time t .

The LDA signal values $LDA(t;ref;j)$ are then provided in an **encrypted** form for the mobile station for a sequence of at least two consecutive times $t=t_1, t_2, \dots, t_n, t_{n+1}, \dots$

USE/ADVANTAGE- GLONAS, LORAN-C systems. Allows temporary cut off of transmission when magnitude of velocity of mobile station is either zero or is below small velocity threshold so eavesdropper has less information to use for decoding **information** contained in **messages** transmitted.

Dwg. 1/7

Terms: SECURE; INFORMATION; COMMUNICATE; METHOD; GROUP; SYSTEM;
TRANSMIT; CORRECT; SIGNAL; CONSECUTIVE; SEQUENCE; TIME; MESSAGE; KEY;
FUNCTION; PRECEDE; CORRECT; VALUE

Derwent Class: W02; W06

International Patent Class (Main): H04K-001/00

International Patent Class (Additional): G01C-021/00; H04B-007/185

File Segment: EPI

16/5/41 (Item 28 from file: 350)

DIALOG(R) File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

011027453 **Image available**

WPI Acc No: 1997-005377/199701

XRPX Acc No: N97-004922

Symmetrical code key delivery system for multimedia communication-
corresp. to ordering and acceptance of goods - has code key generator
which produces symmetrical code key that is shared by first communication
terminal and second communication terminal

Patent Assignee: TOPPAN PRINTING CO LTD (TOPP)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 8274769	A	19961018	JP 9570137	A	19950328	199701 B

Priority Applications (No Type Date): JP 9570137 A 19950328

Details:

Patent No	Kind	Lang	Pg	Main IPC	Filing Notes
JP 8274769	A		8	H04L-009/06	

Abstract (Basic): JP 8274769 A

The system uses two communication terminals (1,2) each with a secret data generator (11,21) which generates first and second secret data (Ra,Rb) respectively. An intermediate key generator (12,22) forms an intermediate key (Xa,Xb) limited by a prime number.

An open key generator (13,23) forms an open key (Ya,Yb) by a primitive soln. multiplied to the intermediate key value.

Communication interfaces (14,24) perform data switching between the communication terminals. A code key generator (15,25) generates a symmetrical code key (K) which is shared by the two communication terminals.

ADVANTAGE - Prevents code key leakage due to function code

key generator. Enables high-speed enciphered data decoding using small-scale hardware due to function of code key.

Dwg.1/2

Title Terms: SYMMETRICAL; CODE; KEY; DELIVER; SYSTEM; COMMUNICATE; CORRESPOND; ORDER; ACCEPT; GOODS; CODE; KEY; GENERATOR; PRODUCE; SYMMETRICAL; CODE; KEY; SHARE; FIRST; COMMUNICATE; TERMINAL; SECOND; COMMUNICATE; TERMINAL

Derwent Class: P85; T01; W01

International Patent Class (Main): H04L-009/06

International Patent Class (Additional): G09C-001/00; H04L-009/14

File Segment: EPI; EngPI

16/5/42 (Item 29 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

010937154 **Image available**

WPI Acc No: 1996-434104/199643

XRPX Acc No: N96-365714

Key encryption method for telecommunications method enabling wire-tapping warrants - defining session key for public and secret keys of monitored and monitoring parties respectively and which is valid for set time interval

Patent Assignee: TELCORDIA TECHNOLOGIES INC (TELC-N); BELL COMMUNICATIONS RES INC (BELL-N)

Inventor: LENSTRA A K; WINKLER P M; YACOBI Y

Number of Countries: 019 Number of Patents: 005

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9628913	A1	19960919	WO 96US2477	A	19960223	199643 B
US 5633928	A	19970527	US 95402176	A	19950310	199727
EP 872064	A1	19981021	EP 96911216	A	19960223	199846
			WO 96US2477	A	19960223	
JP 11502035	W	19990216	JP 96527619	A	19960223	199917
			WO 96US2477	A	19960223	
CA 2215050	C	20001226	CA 2215050	A	19960223	200104
			WO 96US2477	A	19960223	

Priority Applications (No Type Date): US 95402176 A 19950310

Cited Patents: 2.Jnl.Ref; US 5315658; US 5519778

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

WO 9628913 A1 E 29 H04K-001/00

Designated States (National): CA JP

Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE

US 5633928 A 12 H04L-009/00

EP 872064 A1 E H04K-001/00 Based on patent WO 9628913

Designated States (Regional): BE DE FR GB IT NL SE

JP 11502035 W 29 G09C-001/00 Based on patent WO 9628913

CA 2215050 C E H04L-009/14 Based on patent WO 9628913

Abstract (Basic): WO 9628913 A

The method for ensuring limited privacy in a communications network comprises sending from a terminal of a user or party 'a' via a network a cipher text message of the form $c(a,b,d) = F(S(a,b,d),k(a,b,d))$ to a number of parties 'b'.

$P(a)$ is a public key of the party 'a', and $S(a)$ is a secret key of party 'a'. A function $g[S(a)] = P(a) \bmod p$, where p and g are integers. $P(b)$ is a public key of party 'b', and h is a one-way hash function. The term f indicates a has function and d is a time interval. The term $k(a,b,d) = H(S(a),d)$, and

$c(a,b,d) = h(S(a,d), P(b))$, and $k(a,b,d) = h(P(b)[S(a)], d)$ and is a session key valid for a time d .

USE/ADVANTAGE - Facilitates warrants for wire-tapping for bounded time periods. Provides reasonable protection against misuse, greater privacy protection and more effective law enforcement. Can be used to

target certain parties.

Dwg. 1/3

Terms: KEY; **ENCRYPTION**; METHOD; TELECOMMUNICATION; METHOD; ENABLE;
WIRE; TAP; DEFINE; SESSION; KEY; PUBLIC; SECRET; KEY; MONITOR; MONITOR;
PARTY; RESPECTIVE; VALID; SET; TIME; INTERVAL
Derwent Class: P85; W01
International Patent Class (Main): G09C-001/00; H04K-001/00; H04L-009/00;
H04L-009/14
International Patent Class (Additional): H04L-009/08; H04L-009/30;
H04Q-007/38
File Segment: EPI; EngPI

16/5/43 (Item 30 from file: 350)
DIALOG(R) File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

010896607 **Image available**
WPI Acc No: 1996-393558/199639
XRPX Acc No: N96-331584

**Personal information exchange management for ATM network - involves
processing identification information using key code for
encryption derived from parameters**

Patent Assignee: ETA TECHNOLOGIES CORP (ETAT-N)
Inventor: JOHNSON W C; MARX D L
Number of Countries: 070 Number of Patents: 003
Patent Family:

Patent No.	Kind	Date	Applicat No	Kind	Date	Week
WO 9625697	A1	19960822	WO 96US1867	A	19960212	199639 B
AU 9648670	A	19960904	AU 9648670	A	19960212	199705
			WO 96US1867	A	19960212	
US 5689564	A	19971118	US 95388220	A	19950213	199801

Priority Applications (No Type Date): US 95388220 A 19950213
Cited Patents: EP 686905; GB 2144564; US 5249230; WO 9310509
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9625697	A1	E	130	G06F-001/00	

Designated States (National): AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE
DK EE ES FI GB GE HU IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN
MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN

Designated States (Regional): AT BE CH DE DK EA ES FR GB GR IE IT KE LS
LU MC MW NL OA PT SD SE SZ UG

AU 9648670	A			G06F-001/00	Based on patent WO 9625697
US 5689564	A		69	H04L-009/32	

Abstract (Basic): WO 9625697 A

The method involves generating a message. A device file name is retrieved along with a set of identification **information**. A first **key code** is **derived** from parameters. The identification **information** is processed using the first **key code** to **derive** a set of processed identification **information**.

The processing takes place before being sent to the **receiving** device. The identification **information** and the message are **encrypted** using the first **key code**. The device file name, the processed **information** and the **message** are **sent** to the **receiving** device. The device file name is sent to the receiving device in **unencrypted** form.

ADVANTAGE - Provides highly secure user to provider link. Provides inexpensive and generally applicable system.

Dwg. 4b/21

Title Terms: PERSON; INFORMATION; EXCHANGE; MANAGEMENT; ATM; NETWORK;
PROCESS; IDENTIFY; INFORMATION; KEY; CODE; **ENCRYPTION**; DERIVATIVE;
PARAMETER
Derwent Class: T01; T05; W01
International Patent Class (Main): G06F-001/00; H04L-009/32
International Patent Class (Additional): G06F-012/14
File Segment: EPI

16/5/46 (Item 33 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

010314185 **Image available**
WPI Acc No: 1995-215443/199528
XRPX Acc No: N95-168921

Secure non-deterministic public-key encryption system - encrypts
plain text message with public key unique to message receiver for
decryption using private key also used to derive public key
Patent Assignee: RAIKE W M (RAIK-I); RPK NEW ZEALAND LTD (RPKN-N); RPK NZ
LTD (RPKN-N)

Inventor: RAIKE W M

Number of Countries: 060 Number of Patents: 019

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9515633	A1	19950608	WO 94NZ136	A	19941201	199528	B
AU 9512049	A	19950619	AU 9512049	A	19941201	199540	
EP 734624	A1	19961002	WO 94NZ136	A	19941201	199644	
			EP 95903047	A	19941201		
	W	19970930	WO 94NZ136	A	19941201	199749	
			JP 95515543	A	19941201		
NZ 2607128	A	19980427	NZ 277128	A	19941201	199823	
			WO 94NZ136	A	19941201		
US 5799088	A	19980825	WO 94NZ136	A	19941201	199841	
			US 96656185	A	19960923		
AU 702766	B	19990304	AU 9512049	A	19941201	199921	
AU 9911321	A	19990304	AU 9512049	A	19941201	199921	
			AU 9911321	A	19990113		
NZ 329808	A	19990828	NZ 277128	A	19941201	199939	
			NZ 329808	A	19941201		
NZ 336413	A	20000128	NZ 336413	A	19941201	200015	
NZ 336414	A	20000128	NZ 336414	A	19941201	200015	
AU 200053420	A	20001102	AU 9911321	A	19990113	200062	N
			AU 200053420	A	20000816		
AU 200053419	A	20001109	AU 9911321	A	19990113	200063	N
			AU 200053419	A	20000816		
AU 729638	B	20010208	AU 9512049	A	19941201	200113	
			AU 9911321	A	19990113		
AU 750323	B	20020718	AU 9911321	A	19990113	200258	N
			AU 200053419	A	20000816		
AU 750408	B	20020718	AU 9911321	A	19990113	200258	N
			AU 200053420	A	20000816		
JP 3339688	B2	20021028	WO 94NZ136	A	19941201	200278	
			JP 95515543	A	19941201		
JP 2002314534	A	20021025	JP 95515543	A	19941201	200303	
			JP 200237366	A	19941201		
JP 3421950	B2	20030630	WO 94NZ136	A	19941201	200343	
			JP 95515543	A	19941201		

Priority Applications (No Type Date): NZ 260712 A 19940609; NZ 250337 A
19931201; NZ 250475 A 19931216; AU 200053420 A 20000816; AU 200053419 A
20000816

Cited Patents: EP 325238; US 4165444

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

WO 9515633 A1 E 62 H04L-009/30

Designated States (National): AM AT AU BB BG BR BY CA CH CN CZ DE DK EE
ES FI GB GE HU JP KE KG KP KR KZ LK LR LT LU LV MD MG MN MW NL NO NZ PL
PT RO RU SD SE SI SK TJ TT UA US UZ VN

Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT KE LU MC
MW NL OA PT SD SE SZ

AU 9512049 A H04L-009/30 Based on patent WO 9515633

EP 734624 A1 E 62 H04L-009/30 Based on patent WO 9515633

Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LI NL PT
SE

JP 9509748	W	76	G09C-001/00	Based on patent WO 9515633
NZ 277128	A		H04L-009/30	Based on patent WO 9515633
JP 9509748	A		H04K-001/00	Based on patent WO 9515633
JP 9509748	B		H04L-009/30	Previous Publ. patent AU 9512049
				Based on patent WO 9515633
	A		H04L-009/00	Div ex application AU 9512049
				Div ex patent AU 702766
NZ 277128	A		H04L-009/30	Div ex application NZ 277128
				Div ex patent NZ 277128
NZ 336413	A		G06F-007/58	
NZ 336414	A		H04L-009/00	
AU 200053420	A		H04L-009/00	Div ex application AU 9911321
AU 200053419	A		G06F-007/58	Div ex application AU 9911321
AU 729638	B		H04L-009/00	Div ex application AU 9512049
				Div ex patent AU 702766
				Previous Publ. patent AU 9911321
	B		G06F-007/58	Div ex application AU 9911321
				Previous Publ. patent AU 200053419
				Div ex patent AU 729638
AU 750408	B		H04L-009/00	Div ex application AU 9911321
				Previous Publ. patent AU 200053420
				Div ex patent AU 729638
JP 3339688	B2	26	H04L-009/08	Previous Publ. patent JP 9509748
				Based on patent WO 9515633
JP 2002314534	A	29	H04L-009/32	Div ex application JP 95515543
JP 3421950	B2	25	H04L-009/08	Previous Publ. patent JP 9509748
				Based on patent WO 9515633

Abstract (Basic): WO 9515633 A

The secure **encryption** system uses a public **key** is derived from a private key using mathematical operations which are equivalent to exponentiation in finite fields. **Encryption** involves generating a random initialisation **key** which is used to exponentiate the components of the **message receiver**'s public key to produce initial values for a pseudo random binary mixture generator. In addition it is used to compute an open key by exponentiating an initial known generator state.

Cipher text is produced from plain text by clocking the mixture generator from the initial value and combining the output key stream with the plain **text**. The open **key** is also **transmitted**.

Decryption uses the open **key** to set the initial value of another mixture generator.

USE/ADVANTAGE - Authentication of digital signatures. Any attacker is required to compute logarithms over finite fields. Degree of cryptanalytic difficulty is known. High speed operation. High security with minimum length of **ciphertext**. Implementation is simple and efficient.

Dwg.2/5

Title Terms: SECURE; NON; PUBLIC; KEY; **ENCRYPTION**; SYSTEM; PLAIN; TEXT; MESSAGE; PUBLIC; KEY; UNIQUE; MESSAGE; RECEIVE; **DECRYPTER**; PRIVATE; KEY; DERIVATIVE; PUBLIC; KEY

Derwent Class: P85; W01

International Patent Class (Main): G06F-007/58; G09C-001/00; H04K-001/00; H04L-009/00; H04L-009/08; H04L-009/30; H04L-009/32

International Patent Class (Additional): H04K-001/02; H04L-009/06; H04L-009/20; H04L-009/22; H04L-009/24

File Segment: EPI; EngPI

16/5/49 (Item 36 from file: 350)

ALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

009658464 **Image available**

WPI Acc No: 1993-352016/199344

XPX Acc No: N93-271521

Unauthorised data tapping detection process for data transmission system - coding data signature using coupling data transmitted

between transmitter and receiver

Patent Assignee: SIEMENS AG (SIEI); SIEMENS NIXDORF INFORM AG (SIEI)

Inventor: BAUMGAERTNER H; HOFFMANN G; LECHNER S; LECLERC M; LOEHMANN E;

LUKAS K; STEINER F; BAUMGARTNER H; LOHMANN E

Number of Countries: 006 Number of Patents: 005

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9321711	A1	19931028	WO 93DE246	A	19930317	199344 B
EP 635181	A1	19950125	EP 93905200	A	19930317	199508
			WO 93DE246	A	19930317	
EP 635181	B1	19970115	EP 93905200	A	19930317	199708
			WO 93DE246	A	19930317	
DE 59305159	G	19970227	DE 505159	A	19930317	199714
			EP 93905200	A	19930317	
			WO 93DE246	A	19930317	
US 5608800	A	19970304	WO 93DE246	A	19930317	199715
			US 94318700	A	19941011	

Priority Applications (No Type Date): DE 4211989 A 19920409

Cited Patents: EP 117907; EP 197392; US 4281215; US 4578530; US 4853962

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9321711	A1	G	20	H04L-009/00	
EP 635181	A1	G	2	H04L-009/00	Based on patent WO 9321711
EP 635181	B1	G	10	H04L-009/00	Based on patent WO 9321711
Designated States (Regional): CH DE FR GB LI					
DE 59305159	G			H04L-009/00	Based on patent EP 635181
					Based on patent WO 9321711
US 5608800	A		9	H04L-009/08	Based on patent WO 9321711

Abstract (Basic): WO 9321711 A

The detection process assigns the signature to the useful **data** symmetrically **coded** using a **code key dependent** on coupling **data** (K) **transmitted** between the **data transmitter and receiver**. The coupling **data** are combined with random **data provided** by a random generator.

The coupling **data** are **transmitted** uncoded and the random **data** are coded, the coupling **data** pref. being dependent on the **transmission** or reception time for the **data**.

ADVANTAGE - Allows detection of data which have been tapped and fed back into the system with detection of alteration to **transmitted data**.

Dwg.2/4

Title Terms: UNAUTHORISED; DATA; TAP; DETECT; PROCESS; DATA; TRANSMISSION;

SYSTEM; CODE; DATA; SIGNATURE; COUPLE; DATA; TRANSMIT; TRANSMIT; RECEIVE

Derwent Class: W01; W02

International Patent Class (Main): H04L-009/00; H04L-009/08

International Patent Class (Additional): H04K-001/00; H04L-009/14

File Segment: EPI

16/5/51 (Item 38 from file: 350)

INDEX, File 350: Derwent WPIX

© 2004 Thomson Derwent. All rts. reserv.

008889090 **Image available**

WPI Acc No: 1992-016359/199202

XRPX Acc No: N92-012344

Relatively short message encryption for secure communication - combines encrypted selected number and message and sends to second party who has corresp. RSA decryption key and hashing function

Patent Assignee: PITNEY BOWES INC (PITB); PASTOR J (PAST-I)

Inventor: PASTOR J

Number of Countries: 002 Number of Patents: 003

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 5073935	A	19911217	US 90628247	A	19901217	199202 B
CA 2056886	A	19920618	CA 2056886	A	19911204	199236

Priority Applications (No Type Date): US 90628247 A 19901217; US 90628247 A 19901217

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
CA 2056886	A		H04K-001/00	
CA 2056886	C		H04K-001/00	

Abstract (Basic): US 5073935 A

A first party is **provided** with a set of **numbers** that have the property that when **encrypted** using an RSA encryption **key** the resulting set of **encrypted** numbers is of an order substantially smaller than that of the original set. If the **encryption key** and the original set of numbers are of the order of 200 decimal digits then the resulting set of **encrypted** numbers may be of the order of 15-30 decimal digits. To **communicate** a **message** the first party selects a number from the originals set and applies a hashing function to the selected **number** to **obtain** a 64 binary **bit DES key**. The selected number is then **encrypted** with the RSA **key** and a message is **encrypted** with the DES **key** obtained.

The **encrypted** message and the **encrypted** selected number are combined and the combined **message** is **sent** to a second party who has the corresponding RSA **decryption key** and knows the hashing **function**. The second party then **decrypts** the **number**, applies the hashing **function** to **obtain** the DES **key** and **decrypts** the **message**.

USE/ADVANTAGE - Esp. in finance industry for secure transfer of funds. The parties may communicate with substantially the security of RSA while significantly reducing the minimum message length which may be securely **encrypted**. (7pp Dwg.No.2/2)

Title Terms: RELATIVELY; SHORT; MESSAGE; **ENCRYPTION**; SECURE; COMMUNICATE; COMBINATION; **ENCRYPTION**; SELECT; NUMBER; MESSAGE; SEND; SECOND; PARTY; RESPOND; **DECRYPTER**; KEY; HASH; FUNCTION

Patent Class: T01; W01

International Patent Class (Main): H04K-001/00

International Patent Class (Additional): H04L-009/28; H04L-009/30

File Segment: EPI

2/5/54,56,57

16/5/54 (Item 41 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

008475593 **Image available**

WPI App No: 1990-362593/199049

WPIX App No: N90-276654

Coded transmission equipment for public communication system - uses coding appts. at calling and called stations operating with agreed code and authentication arrangement for appropriate security level

Patent Assignee: SIEMENS AG (SIEI)

Inventor: MARKWITZ W

Number of Countries: 016 Number of Patents: 008

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
DE 3919734	C	19901206	DE 3919734	A	19890616	199049 B
WO 9016124	A	19901227				199103
EP 477180	A	19920401	EP 90905428	A	19900405	199214
JP 4506137	W	19921022	JP 90505301	A	19900405	199249
			WO 90DE270	A	19900405	
	A	19930601	WO 90DE270	A	19900405	199323
			US 91793426	A	19911212	
	B1	19940824	EP 90905428	A	19900405	199433
			WO 90DE270	A	19900405	
DE 59006915	G	19940929	DE 506915	A	19900405	199438
			EP 90905428	A	19900405	
			WO 90DE270	A	19900405	
CA 2062751	C	20000808	CA 2062751	A	19900405	200051

Priority Applications (No Type Date): DE 3919734 A 19890616

Cited Patents: EP 205095; EP 307627; EP 48903

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

WO 9016124 A

Designated States (National): CA JP US

Designated States (Regional): AT BE CH DE DK ES FR GB IT LU NL SE

EP 477180 A 24

Designated States (Regional): CH DE DK FR GB LI NL SE

JP 4506137 W 7 H04L-009/06 Based on patent WO 9016124

US 5216715 A 9 H04L-009/02 Based on patent WO 9016124

EP 477180 B1 G 12 H04L-009/32 Based on patent WO 9016124

Designated States (Regional): CH DE DK FR GB LI NL SE

DE 59006915 G H04L-009/32 Based on patent EP 477180

Based on patent WO 9016124

CA 2062751 C E H04K-001/00 Based on patent WO 9016124

Abstract (Basic): DE 3919734 C

The arrangement for **transmitting codes** is intended for a **number** of subscriber stations (TLN A, TLN B), where a **code** is accepted for **communication** between sending and receiving stations. Coding equipment for the agreed **code** is **provided** in the stations which are given a recognition **code**. The **communication** system is equipped with an arrangement for authenticating a subscriber in the **transmissions**.

Depending on the desired degree of security in any transmission, the arrangement can adopt an appropriate checking response. There are two stages or grades of security. The first is intended for speech transmissions and employs a reduced scheme, while the second is more complicated and uses a central station (SMZ) for checking purposes.

USE/ADVANTAGE - Improvement is security for subscriber without undue expense. Suitable for data processing systems. (9pp Dwg.No.2/5

Title Terms: CODE; TRANSMISSION; EQUIPMENT; PUBLIC; COMMUNICATE; SYSTEM; CODE; APPARATUS; CALL; CALL; STATION; OPERATE; AGREE; CODE; AUTHENTICITY; ARRANGE; APPROPRIATE; SECURE; LEVEL

Derwent Class: W01; W02

International Patent Class (Main): H04K-001/00; H04L-009/02; H04L-009/06; H04L-009/32

International Patent Class (Additional): H04B-007/26; H04L-009/08;

H04L-009/14; H04L-012/22; H04Q-007/02

File Segment: EPI

16/5/56 (Item 43 from file: 350)

DIALOG(R) File 350: Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

007666915 **Image available**

WPI Acc No: 1988-300847/198843

XRPX Acc No: N88-228342

Encoding messages in communication network - simplifying key management where unique cryptographic keying relationships are required end-to-end between pairs of parties

Patent Assignee: INT BUSINESS MACHINES CORP (IBM); IBM CORP (IBM)

Inventor: LEE S G; SMITH P R

Number of Countries: 007 Number of Patents: 006

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 287720	A	19881026	EP 87303503	A	19870422	198843 B
JP 63274242	A	19881111				198851
US 4912762	A	19900327	US 88182555	A	19880418	199018
EP 287720	B	19920108				199203
DE 3775924	G	19920220				199209
CA 1315367	C	19930330	CA 564730	A	19880421	199318

Priority Applications (No Type Date): EP 87303503 A 19870422

Cited Patents: 4.Jnl.Ref; WO 8102655

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes
EP 287720 A E 9
Designated States (Regional): DE FR GB IT
EP 287720 B
Designated States (Regional): DE FR GB IT
CA 1315367 C H04L-009/00

Abstract (Basic): EP 287720 A

A first set of nodes **transmits** and **receives** **messages** to and from a second set of nodes, each node in each set having an identification **code** unique to that set. Common cryptographic **keys** are **derived** for each set of nodes. At each node of the first set, the common **key** and a **value** **derived**, dv, from the **encryption** of the **key** are stored with the node identification code.

A **message** **encryption** **key** is **derived** from a combination of the destination node identification **code** **encrypted** by the set common **key** and the stored **derived** **value**, dv, whenever a node of one set has a **message** to **transmit** to a node of the other set.

USE - Network including large population of user terminals which **communicate** with any one of several **data** processing centres.

1/2

Terms: ENCODE; MESSAGE; COMMUNICATE; NETWORK; SIMPLIFY; KEY; MANAGEMENT; UNIQUE; CRYPTOGRAPHIC; KEY; RELATED; REQUIRE; END-TO-END; PAIR; PARTY

Derwent Class: T05; W01

International Patent Class (Main): H04L-009/00

International Patent Class (Additional): G07F-007/10

File Segment: EPI

16/5/57 (Item 44 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

007500575 **Image available**

WPI Acc No: 1988-134508/198820

MRPX Acc No: N88-102370

Enciphering and deciphering digital data signals - has control unit with input connected to text generator and output connected to enciphering unit to provide key

Patent Assignee: PHILIPS GLOEILAMPENFAB NV (PHIG)

Inventor: JANSEN C J

Number of Countries: 014 Number of Patents: 006

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 267647	A	19880518	EP 87202133	A	19871105	198820 B
NL 8602847	A	19880601				198826
AT 8780950	A	19880512				198827
JP 63135035	A	19880607	JP 87284071	A	19871110	198828
US 4890324	A	19891226	US 87118384	A	19871106	199008
CA 1291801	C	19911105				199151

Priority Applications (No Type Date): NL 862847 A 19861111

Cited Patents: A3...8945; EP 105553; No-SR.Pub; US 3796830; US 4157454

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

EP 267647 A E 5

Designated States (Regional): AT BE CH DE FR GB IT LI SE

US 4890324 A 5

Abstract (Basic): EP 267647 A

The data signals to be **enciphered** are processed with aid of a **key** **derived** from a **key** **text**. The nature of the processing operation performed on the data signals to be **enciphered** is determined by an instruction command which is also **derived** from the **key** **text**. The **enciphering** unit (11) has an input (10) for **receiving** clear digital **data** signals. A control arrangement (13) has

an input connected to the key text generator (17) and an output is connected to the **enciphering** unit for providing (14) a **key**.

A second output is connected to the **enciphering** unit for providing (15) the instruction command. The **enciphering** arrangement includes a circuit for **enciphering** a character of the digital data signals under the control of the instruction command and the key character.

ADVANTAGE - Error propagation due to any type of **transmission** errors is prevented, and **number** of processing operations which can be performed on clear text/key combination is large.

22/5/13 (Item 13 from file: 347)
DIALOG(R) File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

05501732 **Image available**

INFORMATION DISTRIBUTION METHOD HIDING CRYPTOGRAPHIC KEY CONTENTS

PUB. NO.: 09-116532 [JP 9116532 A]
PUBLISHED: May 02, 1997 (19970502)
INVENTOR(s): MORIYASU KENJI
AKASHI OSAMU
TERAUCHI ATSUSHI
APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT> [000422] (A Japanese
Company or Corporation), JP (Japan)
APPL. NO.: 07-272521 [JP 95272521]
FILED: October 20, 1995 (19951020)
INTL CLASS: [6] H04L-009/08; G09C-001/00; H04L-009/14
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.9 (COMMUNICATION --
Other)

ABSTRACT

PROBLEM TO BE SOLVED: To **provide** an **information distribution** method where a **sending** terminal sends a cryptographic key that is hidden against other terminals and a receiving terminal and the receiving terminal performs the decoding processing by means of the hidden cryptographic key.

SOLUTION: A sending terminal hides a decoding cryptographic key against other terminals and a receiving terminal and sends this cryptographic key to the receiving terminal. The receiving terminal use the hidden cryptographic **key** to **produce** and carry out a decoding processing application 4. A layer 6 is prepared between a secret communication protocol layer 5 and the application 4 to treat the cryptographic key for the software which is used by the receiving terminal. Thus it is possible to hide the contents of the cryptographic key that contain a function which stores plural cryptographic keys by means of a secret communication protocol, a function which decodes the **cipher information** by means of the cryptographic **keys**, a **function** which erases the cryptographic **keys** out of their treating layer, and a function which shows a cryptographic key identifier to the application 4 for designation of one of these cryptographic keys.

22/5/14 (Item 14 from file: 347)
DIALOG(R) File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

0455917 **Image available**

COMMUNICATION METHOD FOR RADIO COMMUNICATION SYSTEM

PUB. NO.: 05-347617 [JP 5347617 A]
PUBLISHED: December 27, 1993 (19931227)
INVENTOR(s): SHINPO ATSUSHI
OBAYASHI SHUICHI
TSURUMI HIROSHI
OGURA KOJI
APPLICANT(s): TOSHIBA CORP [000307] (A Japanese Company or Corporation), JP
(Japan)
APPL. NO.: 04-154779 [JP 92154779]
FILED: June 15, 1992 (19920615)
INTL CLASS: [5] H04L-009/06; H04L-009/14; H04K-001/00
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 26.2 (TRANSPORTATION --
Motor Vehicles); 44.2 (COMMUNICATION -- Transmission Systems)
; 44.4 (COMMUNICATION -- Telephone)
JOURNAL: Section: E, Section No. 1533, Vol. 18, No. 195, Pg. 23, April
05, 1994 (19940405)

ABSTRACT

PURPOSE: To reduce the communication quantity by devising the method such

that an authentication section authenticates only a radio terminal and a ciphering key between a base station and the radio terminal is shared in common.

CONSTITUTION: A radio terminal sends an authentication number PSi to a base station and the base station generates a random number R1 and sends it to the radio terminal. The radio terminal receives it to generate a random number R2, an authentication information generating means 103 synthesizes the numbers R1, R2 and secret information Sp_{pi} to obtain an authentication number .sigma.ps and it is sent to the base station together with the random number R2. The random numbers R1, R2, the authentication number PSi and the authentication number .sigma.ps are given to an authentication information check means 105, which authenticates the radio terminal as the terminal having the PSi when the result of check is OK, and the radio terminal and the base station generate a common ciphering key by common share means 106a, 106b. Thus, a random number required for mutual authentication consists of key common share information and a function in the device to reduce number of random numbers to be converted thereby reducing the communication quantity.

22/5/19 (Item 5 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

015645716 **Image available**

WFI Acc No: 2003-707899/200367

Related WFI Acc No: 2000-170626; 2001-307087; 2001-595036; 2001-637923;

2002-040302; 2002-054578; 2002-279432; 2002-380635; 2002-391481;

2002-391556; 2003-196892

MRPX Acc No: N03-565588

Displayable data delivery method for distributed processing system, involves encrypting primary digital data using unique key derived from ID label in received data to generate secondary digital data for transmission

Patent Assignee: CHAN H C (CHAN-I)

Inventor: CHAN H C

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 6609202	B1	20030819	US 94224280	A	19940407	200367 B
			US 94255649	A	19940608	
			US 94279424	A	19940725	
			US 96644838	A	19960510	
			US 97939368	A	19970929	
			US 98177681	A	19981022	
			US 2002213394	A	20020805	

Priority Applications (No Type Date): US 98177681 A 19981022; US 94224280 A 19940407; US 94255649 A 19940608; US 94279424 A 19940725; US 96644838 A 19960510; US 97939368 A 19970929; US 2002213394 A 20020805

Patent Details:

Parent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6609202	B1		13	H04L-009/00	CIP of application US 94224280
					CIP of application US 94255649
					CIP of application US 94279424
					CIP of application US 96644838
					CIP of application US 97939368
					Cont of application US 98177681
					CIP of patent US 6021307
					Cont of patent US 6473860

Abstract (Basic): US 6609202 B1

NOVELTY - Two sets of digital data containing the identification (ID) label and having mutual relation is defined and primary data is forwarded to the remote processing units (310,340). The encrypted secondary data is generated by encrypting the primary data using a unique key, after receiving the ID label from the processing units.

The **encrypted data** is transmitted to remaining processing units.

USE - For online **delivery** of displayable **data** in **distributed data** processing system utilized in video **data** , games and television **data distribution** through computer networks.

ADVANTAGE - Unauthorized use of the digital **information** is prevented since the **information providers** control the **encryption** algorithms and **keys** effectively.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the **information distribution** and processing system.

information distribution and processing system (300)

processing units (310,340)

processors (312,314)

output unit (322)

pp; 13 DwgNo 1/4

Title Terms: DISPLAY; DATA; DELIVER; METHOD; DISTRIBUTE; PROCESS; SYSTEM;
PRIMARY; DIGITAL; DATA; UNIQUE; KEY; DERIVATIVE; ID; LABEL; RECEIVE; DATA
; GENERATE; SECONDARY; DIGITAL; DATA; TRANSMISSION

Derwent Class: W01; W04

International Patent Class (Main): H04L-009/00

International Patent Class (Additional): H04N-007/167

Segment: EPI

22/5/41 (Item 27 from file: 350)

FILED(R) File 350:Derwent WPIX

© 2004 Thomson Derwent. All rts. reserv.

012943658 **Image available**

WPI Acc No: 2000-115511/200010

XRPX Acc No: N00-087383

Data decrypting device of data securing medium for protecting digital video disk recordings from home copying and commercial piracy

Patent Assignee: SOFTWARE SECURITY INC (SOFT-N)

Inventor: KULINETS J M

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 6005940	A	19991221	US 97857244	A	19970516	200010 B

Priority Applications (No Type Date): US 97857244 A 19970516

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
US 6005940	A		13 H04L-009/00	

Abstract (Basic): US 6005940 A

NOVELTY - A reader (20) reads **encrypted data** and the unique **decrypting** information stored with each **frame** of **encrypted data** and **transmits** the **decrypting** information to a transponder (2). The transponder includes a **deciphering** engine to **decipher** the **received information** into a **decryption key** , and **transmits** the **key** to the reader. A **decryption** circuit in the reader **decrypts** the read data using the **key** .

DETAILED DESCRIPTION - The unique **decrypting** information is the serial number of the **frame** . An energy coupling circuit **provides** energy to the transponder. The transponder includes a stored data **key** which is combined in algorithm with the **decrypting** information to **derive** the **decryption key** . An INDEPENDENT CLAIM is also included for **data decrypting** method.

USE - For protecting digital video recordings from home copying and commercial piracy.

ADVANTAGE - Offers data medium of **encrypted data** which frustrates the manufacture of illicit copies of the data medium. The non-volatile memory storing secret **deciphering key** is configured to maintain secrecy and avoid an illicit **decryption** of optical disk carrier such as DVD, audio CD or CD-ROM.

DESCRIPTION OF DRAWING(S) - The figure shows a CD-ROM or DVD having self-contained transponder for calculation a **decryption keys** .

Transponder (2)

Reader (20)

pp; 13 DwgNo 1/9

Title Terms: DATA; DEVICE; DATA; SECURE; MEDIUM; PROTECT; DIGITAL; VIDEO;
DISC; RECORD; HOME; COPY; COMMERCIAL; PIRACY
Derwent Class: W01; W04
International Patent Class (Main): H04L-009/00
File Segment: EPI

22/5/42 (Item 28 from file: 350)

DIALOG(R) File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

11943470 **Image available**

Publ No: 2000-115323/200010

Publ No: N00-087208

Encrypted key function processor for executing data transmission
in internet

Patent Assignee: MYTEC TECHNOLOGIES INC (MYTE-N)

Inventor: STOIANOV A; TOMKO G J

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 6002770	A	19991214	US 95508978	A	19950728	200010 B
			US 96584375	A	19960108	
			US 97931028	A	19970915	

Priority Applications (No Type Date): US 97931028 A 19970915; US 95508978 A
19950728; US 96584375 A 19960108

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
US 6002770	A	7	H04L-009/00	CIP of application US 95508978 CIP of application US 96584375 CIP of patent US 5712912 CIP of patent US 5737420

Abstract (Basic): US 6002770 A

NOVELTY - Two characteristic information signals such as fingerprint information signals from users of two remote stations (12,14) are obtained and a sequence of random characters is generated to obtain a **key**. A key function and a Fourier transform of the key to represent the function are obtained.

DETAILED DESCRIPTION - At least one **encrypted** version of the **key** is obtained based on the Fourier transform. One of the two signals is also obtained such that the **key** may be recovered by writing the **encrypted** version to a correlator (21) and inputting either of the two signals to the correlator. The **encrypted** version is stored at each of the two stations, thereafter any message **encrypted** in such a way may be **decrypted** at either of the two stations by retrieving the stored key. **Obtaining** the characteristic **information** signals involves **obtaining** optical beams modulated with biometric images of the fingerprint of the respective users of the first and second stations. The beams are registered in a two-dimensional plane and digitized. **Obtaining** first **information** signal involves **encrypting** the registered beam with a preselected **key** to obtain an **encrypted** first biometric signal and sending it to the second station. The preselected **key** at the second station is utilized to **decrypt** and obtain the **encrypted key** at the second station. **Obtaining key** representing function at the first station involves **encrypting** the function with a preselected **key** and sending the **encrypted** function to the second station. The preselected **key** at the second station is utilized to **decrypt** the function and the **encrypted key** is obtained at the second station.

USE - For executing data transmission in internet.

ADVANTAGE - Provides for secure transmission of data. A different biometric **information** signal such as a vein structure or an iris pattern can be input. The **decryption key** is released only by applying the finger print of the appropriate user.

DESCRIPTION OF DRAWING(S) - The figure shows schematic view of the encrypted key function processor.

Remote stations (12,14)

Correlator (21)

pp; 7 DwgNo 1/2

Title Terms: ENCRYPTION ; KEY; FUNCTION; PROCESSOR; EXECUTE; DATA;

TRANSMISSION

Derwent Class: P85; S05; T01; T02; T04; W01

International Patent Class (Main): H04L-009/00

International Patent Class (Additional): G09C-003/00; H04K-001/00

File Segment: EPI; EngPI

22/5/44 (Item 30 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

012613346 **Image available**

WPI Acc No: 1999-419450/199935

XRPX Acc No: N99-313063

Input vector encrypting system e.g. for secret key cryptosystems

Patent Assignee: HORVATH T (HORV-I); MAGLIVERAS S S (MAGL-I); TRAN V T

(TRAN-I)

Inventor: HORVATH T; MAGLIVERAS S S; TRAN V T

Number of Countries: 082 Number of Patents: 003

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9935776	A2	19990715	WO 98US26454	A	19981211	199935 B
AU 9935444	A	19990726	AU 9935444	A	19981211	199952
US 6038317	A	20000314	US 9768811	A	19971224	200020
			US 9857123	A	19980408	

Priority Applications (No Type Date): US 9857123 A 19980408; US 9768811 P 19971224

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

WO 9935776 A2 E 91 H04L-000/00

Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW

AU 9935444 A H04L-000/00 Based on patent WO 9935776

US 6038317 A H04L-009/28 Provisional application US 9768811

Abstract (Basic): WO 9935776 A2

NOVELTY - The system has a vector acceptor to receive input binary digit vectors and a data key expands pseudo-random number generator receives a user provided input data key, and to generate and output a data key dependent sequence of pseudo-random numbers.

DETAILED DESCRIPTION - A first logarithmic signature container which contains a first logarithmic signature which consisting several mathematical construct blocks. Each mathematical construct block contains two permutations of a sequential number of numbers. A second logarithmic signature container which contains a second logarithmic signature which consists of several mathematical construct blocks. Each mathematical construct block contains two permutations of a sequential number of numbers. A primary mathematical operations accepts a sequence of pseudo-random numbers and accessing the first logarithmic signature container, and accessing the second logarithmic signature container, and applies direction found in a sequence of pseudo-random numbers to a first logarithmic signature caused to be contained in the first logarithmic signature container, to the end that a second logarithmic signature is produced by the primary mathematical operations and caused to be contained in the second logarithmic signature container. A primary factorization device determines, accesses and concatenates into a primary factorization output vector, binary pointers which identify

locations of permutations in a second logarithmic signature caused to be present in the secondary logarithmic signature containing device, which permutations, when sequentially composed, duplicate a vector caused to be input into the primary factorization device. In use a user defined data key is input to the data key expanding pseudo-random number **generator** and the data **key** expanding pseudo-random number generator outputs a sequence of pseudo-random numbers in response. In use the sequence of pseudo-random **numbers** is **received** by the primary mathematical operations and caused to direct alteration of a first logarithmic signature caused to be contained in the first logarithmic signature container, to the end that a second logarithmic signature is produced and caused to be contained in the second logarithmic signature container while preserving a property of logarithmic signatures requiring that they be a collection of ordered mathematical construct blocks in which each input vector **encrypted** by utilization of it can be uniquely represented as one, and only one composition of permutations which are present in the logarithmic signature, one so permutation subjected to composition is selected from each ordered mathematical construct blocks. In use one input vector consisting of a sequence of binary digits, is input, to the primary factorization device from the vector acceptor to receive input binary digit vectors and is utilized by the primary factorization device to determine selection of permutations present in the mathematical construct blocks of the second logarithmic signature which when sequentially composed result in the input vector. In use the primary factorization device assigns identified permutations in each of the mathematical construct blocks of the second logarithmic signature present in the second logarithmic signature container, a binary digit pointer which identifies the permutation location within the second logarithmic signature, and so that in use the primary factorization device further sequentially concatenates the determined binary digit location pointers into a once **encrypted** vector version of the input vector input to the vector acceptor to receive input binary digit vectors and makes the once **encrypted** vector version of the input vector available as output from it. An INDEPENDENT CLAIM is included for a method of **encrypting** input vectors and/or **providing** a sequence of pseudo random **numbers**.

USE - For secret key cryptosystems.

ADVANTAGE - Scalable to any input/output block size 1 and performs **encryption** / **decryption** at very high data rates.

DESCRIPTION OF DRAWING(S) - The figure shows a two stage **encryption** systems sequentially composing factorization and composition devices.

pg: 91 DwgNo 1/11

Terms: INPUT; VECTOR; SYSTEM; SECRET; KEY

Class: W01

International Patent Class (Main): H04L-000/00; H04L-009/28

File Segment: EPI

22/5/50 (Item 36 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

010325545 **Image available**

WPI Acc No: 1995-226819/199530

XRPX Acc No: N95-177761

Communication method between network entities using encryption key - delivering information pieces for deriving encryption keys to each entity and corresp. to all entity pairs including that entity

Patent Assignee: CANON KK (CANO)

Inventor: IWAMURA K; YAMAMOTO T

Number of Countries: 019 Number of Patents: 006

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 660565	A2	19950628	EP 94309566	A	19941220	199530 B
JP 7181892	A	19950721	JP 93346642	A	19931222	199538
EP 660565	A3	19960327	EP 94309566	A	19941220	199624

EP 660565	B1	19990825	EP 94309566	A	19941220	199939
DE 69420239	E	19990930	DE 620239	A	19941220	199946
			EP 94309566	A	19941220	
US 5966449	A	19991012	US 94359636	A	19941220	199949

Priority Applications (No Type Date): JP 93346642 A 19931222
 Cited Patents: -SR.Pub; 2.Jnl.Ref; EP 123360; XEP 207534; AJP04150428
 Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 660565	A2	E	19	H04L-009/08	
Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LI LU MC					
NL PT SE					
EP 660565	A		11	G09C-001/10	
EP 660565	B1	E		H04L-009/08	
Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LI LU MC					
NL PT SE					
DE 69420239	E			H04L-009/08	Based on patent EP 660565
EP 660565	A3			H04L-009/08	
US 5966449	A			H04L-009/00	

Abstract (Basic): EP 660565 A

The **communication**. method involves creating pieces of **information** at a network centre, pref. random numbers, independent for every combination of two network entities. The centre **delivers** to each entity the random **numbers** corresp. to combinations involving the entity. A **sender** entity selects the **delivered** random **number** corresp. to the combination including the destination entity.

The **sender** entity **encrypts** **communication** **text** using an **encryption** **key** **determined** from the selected random number. The destination entity selects the random number corresp. to the combination of itself and the sender entity. It uses it to **determine** an **encryption** **key** for **decrypting** the **received** **cipher** **text**.

USE/ADVANTAGE - Enables simple and safe **encryption** **key** sharing without preliminary communication between entities. Secret keys are safe against collusion between entities.

Dwg.1/7

Title Terms: COMMUNICATE; METHOD; NETWORK; ENTITY; **ENCRYPTION** ; KEY; DELIVER; INFORMATION; PIECE; DERIVATIVE; **ENCRYPTION** ; KEY; ENTITY; CORRESPOND; ENTITY; PAIR; ENTITY

International Class: P85; W01

International Patent Class (Main): G09C-001/10; H04L-009/00; H04L-009/08

International Patent Class (Additional): G06F-013/00; H04L-009/06;

H04L-009/14

File Segment: EPI; EngPI

22/5/51 (Item 37 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

010314181 **Image available**

WPI Acc No: 1995-215439/199528

WPI Acc No: N95-168917

Secure communication with encryption key determination over non-secure link - providing stations with seed keys and using two-part data encryption key based on pointer values randomly selected at both stations

Patent Assignee: CREST IND INC (CRES-N)

Inventor: HOSKINSON J D

Number of Countries: 059 Number of Patents: 003

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9515629	A1	19950608	WO 94US13783	A	19941201	199528 B
AU 9513332	A	19950619	AU 9513332	A	19941201	199540
US 5455862	A	19951003	US 93160897	A	19931202	199545

Priority Applications (No Type Date): US 93160897 A 19931202

Cited Patents: US 5193114; US 5297207

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

WO 9515629 A1 E 31 H04K-001/00

Designated States (National): AM AT AU BB BG BR BY CA CH CN CZ DE DK EE
ES FI GB GE HU JP KE KG KP KR KZ LK LR LT LU LV MD MG MN MW NL NO NZ PL
PT RO RU SD SE SI SK TJ TT UA UZ VN

Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT KE LU MC
MW NL OA PT SD SE SZ

AU 9513332 A H04K-001/00 Based on patent WO 9515629

US 5455862 A 16 H04L-009/00

Abstract (Basic): WO 9515629 A

The method for establishing secure communication between two stations involves providing a set of stored seed **keys** to the linked **encryption / decryption** units (EDUs). Each EDU randomly generates pointers which determine the number of times that a loop is repeated in which values are logically combined and **encrypted**, using one of the seed **keys** to determine a portion of the data **encryption key**.

An **encrypted key** header is **produced** and transmitted to the other EDU. The header is **decrypted** by the receiving EDU and its pointer used to determine the portion of the data **encryption key** **developed** by the other EDU. The two portions are then logically combined at each EDU to produce the final DEK and permit secure **data exchange** to take place. Pref., each station is provided with three identical seed keys.

USE/ADVANTAGE - Allows secure transmission to be achieved over non-secure communication link without explicit **transfer** of key **data** or use of public key.

Dwg.2/6

Title Terms: SECURE; COMMUNICATE; **ENCRYPTION** ; KEY; DETERMINE; NON; SECURE ; LINK; STATION; SEED; KEY; TWO; PART; DATA; **ENCRYPTION** ; KEY; BASED; POINT; VALUE; RANDOM; SELECT; STATION

Derwent Class: W01

International Patent Class (Main): H04K-001/00

International Patent Class (Additional): H04L-009/00

File Segment: EPI

22/5/53 (Item 39 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

010159932 **Image available**

WPI Acc No: 1995-061185/199508

WPIX Acc No: N95-048627

Subscriber unit to authenticate communications in real time - uses encryption process with packetised message encryption key and unique packet number as encryption variables

Assignee: MOTOROLA INC (MOTI)

Inventor: BROWN D P; FINKELSTEIN L D; SMOLINSKE J C

Number of Countries: 022 Number of Patents: 009

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9501684	A1	19950112	WO 94US5726	A	19940423	199508	B
FI 9500714	A	19950217	WO 94US5726	A	19940423	199520	
			FI 95714	A	19950217		
EP 663124	A1	19950719	EP 94919195	A	19940423	199533	
			WO 94US5726	A	19940423		
US 5455863	A	19951003	US 9384664	A	19930629	199545	
JP 8500950	W	19960130	WO 94US5726	A	19940423	199642	
			JP 95503476	A	19940423		
US 5689563	A	19971118	US 9384664	A	19930629	199801	
			US 95457212	A	19950601		
CA 2141318	C	19981229	CA 2141318	A	19940423	199911	
KR 181566	B1	19990515	WO 94US5726	A	19940423	200053	
			KR 95700812	A	19950228		
MX 204360	B	20010926	MX 944953	A	19940629	200246	

Priority Applications (No Type Date): US 9384664 A 19930629; US 95457212 A 19950601

Cited Patents: US 5077790; US 5091942

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

WO 9501684 A1 E 254 H04L-009/32

Designated States (National): CA FI JP KR

Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE

FI 9500714 A H04L-000/00

EP 663124 A1 E 254 H04L-009/32 Based on patent WO 9501684

Designated States (Regional): DE FR GB NL SE

JP 455863 A 13 H04L-009/32

JP 455863 W 26 H04L-009/00 Based on patent WO 9501684

JP 455863 A 10 H04L-009/32 Cont of application US 9384664

Cont of patent US 5455863

JP 455863 A 10 H04L-009/32

JP 455863 A 10 H04L-009/32

JP 455863 A 10 H04L-009/32

JP 455863 A 10 H04L-009/32

Abstract (Basic): WO 9501684 A

The subscriber unit has a memory which contains an identifier for the unit, two items of shared-secret data, a random challenge, and instant-specific information. A processor is coupled to the memory for generating an authentication message as a function of the first shared-secret data, the random challenge, and the instant specific information.

A **key generator** is coupled to the memory to **generate** a session **key** as a **function** of the two shared secret **data**, the random challenge and the instant specific information. An **encrypting** unit is coupled to the **key generator** to **encrypt** dialled digits identifying a target communication unit, using the session **key** as an **encryption** variable. A transmitter is connected to the memory, the processor and the **key generator** for **transmitting** in a single **message** the first subscriber identifier, the authentication message and the **encrypted** data.

USE/ADVANTAGE - Radio telephone and paging systems. Provides efficient real time authentication method and appts. using single **message** to **provide** authentication and **communication** link set-up information .

Dwg.1/5

Title Terms: SUBSCRIBER; UNIT; AUTHENTICITY; COMMUNICATE; REAL; TIME; ENCRYPTION ; PROCESS; MESSAGE; ENCRYPTION ; KEY; UNIQUE; PACKET; NUMBER; ENCRYPTION ; VARIABLE

Derwent Class: P85; W01

International Patent Class (Main): G09C-001/00; H04L-000/00; H04L-009/00; H04L-009/32

International Patent Class (Additional): H04B-001/69; H04K-001/00; H04L-009/10; H04L-009/12; H04Q-007/38

File Segment: EPI; EngPI

22/5/57 (Item 43 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

000033307 **Image available**

WI Acc No: 1992-160663/199220

KREFX Acc No: N92-120484

Secure communication system deriving key from received information - encrypts information to be transmitted from between appts.

utilising key information signal received from information memory

Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE); NITTO CHEM IND CO LTD (NITT)

Inventor: KUMAZAKI K; MANO F; MIKI N; OKADA K; TOKURA N

Number of Countries: 005 Number of Patents: 007

Patent Family:

Patent No Kind Date Applicat No Kind Date Week

EP 484862	A	19920513	EP 91118788	A	19911104	199220	B
JP 5007202	A	19930114	JP 91288717	A	19911105	199307	
US 5204903	A	19930420	US 91786799	A	19911105	199317	
EP 484862	A3	19930310	EP 91118788	A	19911104	199349	
EP 484862	B1	19970416	EP 91118788	A	19911104	199720	
DE 69125685	E	19970522	DE 625685	A	19911104	199726	
			EP 91118788	A	19911104		
JP 3008965	B2	20000214	JP 91288717	A	19911105	200013	

Priority Applications (No Type Date): JP 90299492 A 19901105

Cited Patents: No-SR.Pub; 1.Jnl.Ref; EP 353352; US 4926478

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing	Notes
-----------	------	-----	----	----------	--------	-------

EP 484862	A	E	27			
-----------	---	---	----	--	--	--

Designated States (Regional): DE FR GB

JP 3008965	B2	22	H04L-009/16	Previous Publ. patent JP 5007202
------------	----	----	-------------	----------------------------------

US 5204903	A	23	H04L-009/02
------------	---	----	-------------

EP 484862	B1 E	33	H04L-009/18
-----------	------	----	-------------

Designated States (Regional): DE FR GB

DE 69125685	E		H04L-009/18	Based on patent EP 484862
-------------	---	--	-------------	---------------------------

JP 5007202	A		H04L-009/28
------------	---	--	-------------

Basic): EP 484862 A

The communication system includes two pieces of communication appts. (100A, 100B) interconnected via a transmission medium, e.g. line (10L). Both appts. have transmit (12A, 12B) and receive (13A, 13B) circuits. One has a conversion circuit (17A) for **encrypting** an **information** signal to be **transmitted** (A) to the second utilising a signal (B') received from it.

The second appts. has an information memory (23B) for storing as key **information**, **information** (B) it **transmits** to the first appts. It also has an inverse conversion circuit (18B) for decoding a received **encrypted** signal (A') using the **key** information read out of information memory.

ADVANTAGE - Key **information** varies with **transmitted** signal from which it is derived, providing highly secure communication system. Simple construction.

File 348:EUROPEAN PATENTS 78-2004/Mar W01

(c) 2004 European Patent Office

File 349:PCT FULLTEXT 1979-2002/UB=20040311,UT=20040304

(c) 2004 WIPO/Univention

Set	Items	Description
S1	313571	MESSAGE? ? OR EMAIL OR MAIL OR TEXT OR CODE? ?
S2	13110	KEY? ?(5N) (DEPENDENT OR DEPENDENCE OR RELIAN?? OR CONTINGENT OR FUNCTION OR DERIV???)
S3	110073	S1(5N) (SEND??? OR SENT OR TRANSMIT? OR TRANSFER???? OR TRANSMISSION OR FORWARD??? OR RELAY??? OR CONVEY? OR DELIVER??? - OR COMMUNICAT? OR EXCHANG? OR BROADCAST??? OR DISTRIBUT??? OR RECEIV?)
S4	28210	CIPHER? OR CYPHER? OR ENCRYPT? OR ENCIPHER? OR ENCYIPHER? OR DECRYPT? OR DECIPHER? OR DECYIPHER? OR UNENCIPHER? OR UNENCRYPT? OR UNCIPHER?
S5	3689	SHARED(1W) (KEY OR DATA OR INFORMATION OR VALUE? ? OR NUMBER? ? OR CODE? ?).
S6	20527	KEY(3N) (ESTABLISH? OR GENERAT? OR CREAT???? OR FASHION? OR CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR PRODUC????? OR DEVELOP? OR BUILT OR BUILD?)
S7	11412	KEY(5N) (COMPUTE OR COMPUTES OR COMPUTED OR COMPUTING OR DETERMIN? OR DISCERN? OR DERIV? OR CALCULA?)
S8	1497	S2(7N)S1
S9	10192	KEY(5N)S4
S10	177	S8(50N)S9(50N)S3
S11	146	S8(30N)S9(30N)S3
S12	48	S11/AB,CM
S13	19	S8(50N)S9(50N)S5
S14	15	S13 NOT S12
S15	138	S8(30N)S9(30N)S3(30N)S6:S7
S16	78	S8(30N)S9(30N)S3(30N)S6
S17	44	S16 NOT (S12 OR S14)
S18	60	S11 NOT (S12 OR S14 OR S17)
S19	17	S10 NOT (S12 OR S14 OR S17 OR S18)

00416791 **Image available**

DATA ENCRYPTION

CODAGE DE DONNEES

Patent Applicant/Assignee:

FARIA Richard Steven,

Inventor(s):

FARIA Richard Steven,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9807252 A1 19980219

Application: WO 97GB2138 19970811 (PCT/WO GB9702138)

Priority Application: GB 9616803 19960809

Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES

FI GB GE GH HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN

MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU

ZW GH KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES

FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD

TG

Publication Language: English

Fulltext Word Count: 1671

Fulltext Availability:

Claims

Claim

1, A system for transmitting digital data to a plurality of users on demand, each user having an associated unique identity **code**, the system comprising means for **receiving** 5 from a user that user's identity code together with a demand for specified digital data and, in response thereto, encrypting the demanded data, using as an **encryption key** a **function** of that user's unique identity **code**, and **transmitting** the encrypted data to the user,

2 A system as claimed in claim 1, wherein the **encryption key** is identical to the **received** unique identity **code**.

3 A system as claimed in claim 1 or claim 2, wherein each user's unique identity code represents credit card data.

4 A system...

...second sequence of bits by individually transforming each bit of said first sequence into a corresponding bit of said second sequence in dependence on said **encryption key**.

5 A method of transmitting digital data to a plurality of users on demand,, each user having an associated unique identity **code**, the method comprising **receiving** from a user that user's identity code together with a demand for specified digital data and, in response thereto, encrypting the demanded data, using as an **encryption key** a **function** of that user's unique identity **code**, and **transmitting** the encrypted data to the user.

6 A method as claimed in claim 5, wherein the **encryption key** is identical to the **received** unique identity **code**.

7 A method as claimed in claim 5 or claim 6, wherein each user's unique identity code represents credit card data.

8 A method...

00376159

UNIFIED END-TO-END SECURITY METHODS AND SYSTEMS FOR OPERATING ON INSECURE NETWORKS

PROCEDES ET SYSTEMES UNIFIES PRESENTANT UNE SECURITE DE BOUT EN BOUT ET SERVANT A UNE EXPLOITATION SUR DES RESEAUX NON SURS

Patent Applicant/Assignee:

TRI-STRATA SECURITY INC,

Inventor(s):

ATALLA Martin M,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9716902 A2 19970509

Application: WO 96US17479 19961101 (PCT/WO US9617479)

Priority Application: US 9529 19951102

Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES

FI GB GE HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW

MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN KE LS MW SD

SZ UG AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU

MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG

Publication Language: English

Fulltext Word Count: 23564

Fulltext Availability:

Fulltext

Claim

... to allow the
sender to identify from the master signature said
second subset of bytes; and
using said second subset of bytes to encrypt
the **message** at the sender and when the encrypted
message is received at the receiver, to decrypt
the received message at the receiver.

19 The method of...

...step of
using said second subset of bytes to encrypt the
message at the sender and to decrypt the received
message at the receiver comprises:
deriving an **encryption key** at both said
sender and said receiver from said subset of
bytes;
encrypting at the sender the message to be
sent to the receiver using said **encryption key** ;
sending said **encrypted message** to the
receiver ; and
decrypting the **received message** using the
encryption key originally generated at the
receiver, whereby the second subset of bytes from
which the **encryption key** is derived is never
transmitted between the sender and the receiver.

20 The method of generating an encryption key
for use in encrypting information to...said second subset of bytes to
encrypt the
message at the sender and said means for using said
second subset of bytes to decrypt the **received message**
at the receiver comprise:
means for deriving an **encryption key** at said
sender from said subset of bytes;
means for deriving the same **encryption key** at
said receiver from said subset of bytes;
means for encrypting at the sender the
message to be sent to the receiver using said
encryption key ;
means for sending said **encrypted message** to

the receiver; and
means for decrypting the received message
using the encryption key derived at the receiver,
whereby the second subset of bytes from which the
encryption key is derived is never transmitted
between the sender and the receiver.

64 Structure for generating an encryption key
for use in encrypting information to be transmitted
from a sender to a receiver which comprises:
means for generating a master signature
associated with a sender;
means for storing...

12/3,K/44 (Item 25 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00346400

KEY ESCROW METHOD WITH WARRANT BOUNDS
PROCEDE DE REMISE EN MAINS TIERCES D'UNE CLE DE CODAGE AVEC LIMITES
SPECIFIEES PAR LE MANDAT

Patent Applicant/Assignee:

BELL COMMUNICATIONS RESEARCH INC,

Inventor(s):

LENSTRA Arjen Klaas,

WINKLER Peter Mann,

YACOBI Yacov,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9628913 A1 19960919

Application: WO 96US2477 19960223 (PCT/WO US9602477)

Priority Application: US 95402176 19950310

Designated States: CA JP AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE

Publication Language: English

Fulltext Word Count: 6802

Fulltext Availability:

Claims

Claim

... a one way hash

function;

(b) providing to a wiretapper terminal connected to
said network sufficient information to permit said
wiretapper terminal to decrypt said cipher message
using said cipher key and obtain said session key
without said wiretapper terminal obtaining said
secret key of the party a;

(c) transmitting an information message via said
network between said parties a and b encrypted using
said cipher function f and said session key ; and
20

(d) decrypting said information message transmitted
between said parties a and b at said wiretapper
terminal.

4 The method of claim 3, wherein:

said session key is determined by a processing...

12/3,K/45 (Item 26 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00343185

Image available

PERSONAL ACCESS MANAGEMENT SYSTEM

SYSTEME DE GESTION D'ACCES PERSONNEL

Patent Applicant/Assignee:

ETA TECHNOLOGIES CORPORATION,
Inventor(s):

JOHNSON William Cedric,
MARX Donald L,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9625697 A1 19960822

Application: WO 96US1867 19960212 (PCT/WO US9601867)

Priority Application: US 95388220 19950213

Designated States: AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB

GE HU IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL

PT RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN KE LS MW SD SZ UG AZ BY

KG KZ RU TJ TM AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE BF BJ CF

CU CI CM GA GN ML MR NE SN TD TG

Publication Language: English

Fulltext Word Count: 43795

Fulltext Availability:

Claims

Claim

... said device file name and said set of identification information;
deriving a first key code from said parameters;
processing said identification information using said first **key code**
to **derive** a set of
processed identification information; and
sending said device file name, said processed identification information,
and said **message** to the **receiving** device.

2. The method of claim 1, wherein said message is processed using said
first **key code** 15 prior to being **sent** to the receiving device.

3. The method of claim 2, wherein said identification information and said
message are **encrypted** using said first **key code** as an **encryption**
key.

4. The method of claim 3, wherein said device file name is sent to the
receiving device in unencrypted form.

5. The method of claim...

12/3,K/46 (Item 27 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00268335 **Image available**

SOFTWARE EVALUATION AND DISTRIBUTION APPARATUS, SYSTEM, AND METHOD
PROCEDE, SYSTEME ET APPAREIL D'EVALUATION ET DE DISTRIBUTION DE LOGICIELS

Patent Applicant/Assignee:

INFONOW CORPORATION,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9416508 A1 19940721

Application: WO 94US97 19940106 (PCT/WO US9400097)

Priority Application: US 931262 19930107

Designated States: AU CA JP NZ AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT

SE

Publication Language: English

Fulltext Word Count: 24805

Fulltext Availability:

Claims

Claim

... key.

15. The system of claim 39, wherein:
the encrypting means is additionally for dividing the key into a partial
key and a complementary partial **key**, and for **encrypting** the

complementary

partial **key** to provide an **encrypted** partial **key** ;

the distributing means is additionally for distributing the **encrypted** partial **key** to the users;

the key storing means is for storing the partial key;

the coding means is for coding the partial key, using the user identification, to provide a coded partial key;

the central communication means transmits the return **message** including the coded partial key;

the key decoding means is for **deriving** the key from the **coded** partial **key** and the **encrypted** partial **key** , and includes:

a partial key decoding means for decoding the coded partial key to provide a partial **key** ,

a means for **decrypting** the **encrypted** partial **key** to provide the complementary partial key, and

a means for combining the partial key and the complementary partial key to provide the key.

.....

12/3,K/47 (Item 28 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2004 WIPO/Univentio. All rts. reserv.

00156314

SIGNAL PROCESSING APPARATUS AND METHODS

DISPOSITIF ET PROCEDES DE TRAITEMENT DE SIGNAUX

Patent Applicant/Assignee:

HARVEY John C,

Inventor(s):

HARVEY John C,

CUDDIHY James W,

Patent and Priority Information (Country, Number, Date):

Patent: WO 8902682 A1 19890323

Application: WO 88US3000 19880908 (PCT/WO US8803000)

Priority Application: US 8796 19870911

Designated States: AT AU BE BJ BR CF CG CH CM DE DK FI FR GA GB GB HU IT JP

KP LK LU MC MG ML MR MW NL NO RO SE SN SU TD TG

Publication Language: English

Fulltext Word Count: 161690

Fulltext Availability:

Claims

File

... 001

... facilities meters (262 in Fig. 7)e

examples of controlled functions include:

1 0

Load and run the contents of the information segment.

Decrypt the execution segment using **decryption key** Go

Decrypt the execution and meter-monitor segments using

decryption key Jo

Commence the video overlay combining designated in the meter-monitor segment.

Modify the execution segment to instruct URS

microcomputer, 205, to commence overlay designated...

12/3,K/48 (Item 29 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2004 WIPO/Univentio. All rts. reserv.

00134707

Image available

METHOD AND APPARATUS FOR SCRAMBLING AND DESCRAMBLING TELEVISION SIGNALS

PROCEDE ET APPAREIL DE BROUILLAGE ET DE DEBROUILLAGE DE SIGNAUX DE TELEVISION

Patent Applicant/Assignee:

SCIENTIFIC ATLANTA INC,

Inventor(s):

LUCAS Keith,

Patent and Priority Information (Country, Number, Date):

Patent: WO 8607224 A1 19861204

Application: WO 86US801 19860421 (PCT/WO US8600801)

Priority Application: US 85599 19850524

Designated States: AT AU BB BE BG BR CH CH DE DE DK FI FR GB GB HU IT JP

KP KR LK LU LU MC MG MW NL NL NO RO SD SE SE SU

Publication Language: English

Full Text Word Count: 6160

Full Text Availability:

Full Text

Claim

... accordance with video

scrambling codes;

providing video descrambling codes for descrambling said

scrambled video information;

encrypting said video descrambling codes in accordance

with a first **encryption** key;

with

providing a session key for decrypting said encrypted video

descrambling codes;

encrypting said session **key** in accordance with a second

encryption **key** ;

including said **encrypted** video descrambling codes and said

encrypted session **key** in said television- during said second period

during

which no video information is present; and

providing a subscriber code and a fixed key at the

receiver which receives said television signal, said subscriber code and

said fixed key being used to derive a distribution key, said distribution

key being used to **decrypt** said **encrypted** session key; said

decrypted

session **key** being used to **decrypt** said **encrypted** video descramble

codes,, said **decrypted** video descramble codes being used to descramble

said scrambled video information.

30s The method of claim 29 wherein said step of providing a

session- **key** includes the step of deriving said session **key** from said

first **encryption** **key** *

31a The method of claim 29 wherein said session key is

changed periodically.

32e The method of claim 29 wherein the step of providing a...

...a plurality of validation codes, each of said plu

rality of validation codes being unique for each of said receivers which

receives said television signal;

encrypting said session -key in accordance -with a second

encryption key;

transmitting said encrypted video descrambling codes, said

AE

encrypted session key and said plurality of...plurality of

validation codes, said comparator providing a logic signal indication

when a match is found, said logic signal enabling logic means to

permit said **decrypted** session **key** to **decrypt** said **encrypted** video

descramble codes, said **decrypted** video descramble codes being used to

descramble said scrambled video information.

34o The method of claim 33 wherein said step of providing a

session **key** for **decrypting** said **encrypted** video descrambling **codes**

includes the step of **deriving** said session **key** from said first

encryption **key** .

35o The method of claim 33 wherein the step of providing a

distribution key at said receiver includes the step of deriving said

distribution **key** from said **encryption** **key** .

14/3,K/1 (Item 1 from file: 348)
DIALOG(R) File 348:EUROPEAN PATENTS
© 2004 European Patent Office. All rts. reserv.

01694847

Methods, apparatus and framework for purchasing of goods and services
Verfahren, Vorrichtung und Gerüst zum Einkaufen von Waren und
Dienstleistungen

Procede, appareil et cadre pour l'achat de biens et de services

PATENT ASSIGNEE:

FUJITSU LIMITED, (211463), 1-1, Kamikodanaka 4-chome, Nakahara-ku,
Kawasaki-shi, Kanagawa 211-8588, (JP), (Applicant designated States:
all)

INVENTOR:

Labrou, Yannis, Fujitsu Laboratories of America 8400 Baltimore Ave,
College Park, MD 20862, (US)
Ji, Lusheng, Fujitsu Laboratories of America 8400 Baltimore Ave, College
Park, MD 20862, (US)
Agre, Jonathan Russell, Fujitsu Laboratories of America 8400 Baltimore
Ave, College Park, MD 20862, (US)

LEGAL REPRESENTATIVE:

Hitching, Peter Matthew et al (74872), Haseltine Lake, Imperial House,
15-19 Kingsway, London WC2B 6UD, (GB)

PATENT (CC, No, Kind, Date): EP 1388797 A2 040211 (Basic)

APPLICATION (CC, No, Date): EP 2003254927 030807;

PRIORITY (CC, No, Date): US 401807 P 020808; US 458205 030611; US 628569
030729; US 628584 030729; US 628583 030729

DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR;
HU; IE; IT; LI; LU; MC; NL; PT; RO; SE; SI; SK; TR

EXTENDED DESIGNATED STATES: AL; LT; LV; MK

INTERNATIONAL PATENT CLASS: G06F-017/60

ABSTRACT WORD COUNT: 144

NOTE:

Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200407	2900
SPEC A	(English)	200407	38754
Total word count - document A			41654
Total word count - document B			0
Total word count - documents A + B			41654

14/3,K/2 (Item 2 from file: 348)
DIALOG(R) File 348:EUROPEAN PATENTS
© 2004 European Patent Office. All rts. reserv.

01694846

Secure communications

Gesicherte Kommunikationen

Communications securisees

PATENT ASSIGNEE:

FUJITSU LIMITED, (211462), 1015, Kamikodanaka, Nakahara-ku, Kawasaki-shi,
Kanagawa 211-8588, (JP), (Applicant designated States: all)

INVENTOR:

Labrou, Yannis, Fujitsu Laboratories of America, 8400 Baltimore Avenue
Suite 302, College Park, MD 20862, (US)
Ji, Lusheng, Fujitsu Laboratories of America, 8400 Baltimore Avenue Suite
302, College Park, MD 20862, (US)
Agre, Jonathan R., Fujitsu Laboratories of America, 8400 Baltimore Avenue
Suite 302, College Park, MD 20862, (US)

LEGAL REPRESENTATIVE:

Hitching, Peter Matthew et al (74871), Haseltine Lake & Co., Imperial
House, 15-19 Kingsway, London WC2B 6UD, (GB)

PATENT (CC, No, Kind, Date): EP 1388991 A2 040211 (Basic)

APPLICATION (CC, No, Date): EP 2003254926 030807;

STIC Search Results (2/2)

PRIORITY (CC, No, Date): US 401807 P 020808; US 458205 030611
DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR;
HU; IE; IT; LI; LU; MC; NL; PT; RO; SE; SI; SK; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK
INTERNATIONAL PATENT CLASS: H04L-029/06; H04L-012/22
ABSTRACT WORD COUNT: 60
NOTE:

Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200407	3409
SPEC A	(English)	200407	11756
Total word count - document A			15165
Total word count - document B			0
Total word count - documents A + B			15165

...SPECIFICATION preferably known only to the device and the verification party, but if generally known are not sufficient to determine the key, without knowledge of the **shared secret value**. The secret value, or the stored parameters, or the key are never transmitted in a message. What is transmitted is a **message** parts of which are **encrypted** with a **key** that is **derived** from the stored parameters and the **shared secret information** that is input by the user.
Another aspect of the present invention relates to a computer program which, when run on a computer system, causes...

14/3,K/3 (Item 3 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01409274

Method and device for performing secure transactions
Verfahren und Vorrichtung zur Ausführung von gesicherten Transaktionen
Procede et dispositif de realisation de transactions securisees
PATENT ASSIGNEE:

Vericom Corp., (2118052), 5520 Explorer Drive, 4th Floor, Mississauga,
Ontario L4W 5L1, (CA), (Applicant designated States: all)

INVENTOR:

Worcks, Timothy, 21 Saturn Street, San Francisco, California 95112, (US)

LEGAL REPRESENTATIVE:

Coyle, Philip Aidan et al (72291), F. R. KELLY & CO. 27 Clyde Road
Ballsbridge, Dublin 4, (IE)

PATENT (CC, No, Kind, Date): EP 1191743 A2 020327 (Basic)
EP 1191743 A3 030917

APPLICATION (CC, No, Date): EP 2001650107 010920;

PRIORITY (CC, No, Date): US 665763 000920

DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI;
LU; MC; NL; PT; SE; TR

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: H04L-009/32

ABSTRACT WORD COUNT: 120

NOTE:

Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200213	460
SPEC A	(English)	200213	5310
Total word count - document A			5770
Total word count - document B			0
Total word count - documents A + B			5770

...SPECIFICATION trusted provider of certificate status information.
Hereafter, certificate status queries and responses can be sent over the

secure connection, each being symmetrically authenticated with the shared secret key negotiated in the handshake phase of establishing the secure connection. In protocols such as SSL, these symmetrically authenticated messages may be transmitted over several connections, each deriving its keys from a single shared secret established in an initial handshake. This use of a secure connection instead of individually authenticated messages gains a performance advantage...

14/3,K/4 (Item 4 from file: 348)
DIALOG(R) File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01364322

System, apparatus and method for presentation and manipulation of syntax objects

System, Vorrichtung und Verfahren zur Vorstellung und Manipulation von Syntaxobjekten

Système, appareil et méthode pour la présentation et la manipulation d'objets syntaxiques

PATENT ASSIGNEE:

International Business Machines Corporation, (200128), New Orchard Road, Armonk, NY 10504, (US), (Applicant designated States: all)

INVENTOR:

Yarsa, Julianne, c/o IBM UK Ltd Intel.Prop.Law MP 110, Hursley Park, Hursley Winchester, Hampshire SO21 2JN, (GB)

Nadalin, Anthony, c/o IBM UK Ltd Intel.Prop.Law MP 110, Hursley Park, Hursley Winchester, Hampshire SO21 2JN, (GB)

Rich, Bruce A., c/o IBM UK Ltd Intel.Prop.Law MP 110, Hursley Park, Hursley Winchester, Hampshire SO21 2JN, (GB)

Shrader, Theodore Jack London, c/o IBM UK Ltd Intel.Prop.Law MP110, Hursley Park, Hursley Winchester, Hampshire SO21 2JN, (GB)

LEGAL REPRESENTATIVE:

Barry, Roger James, Dr. et al (52152), IBM United Kingdom Limited Intellectual Property Department Hursley Park, Winchester Hampshire SO21 2JN, (GB)

PATENT (CC, No, Kind, Date): EP 1162530 A2 011212 (Basic)

APPLICATION (CC, No, Date): EP 2001000132 010430;

PRIORITY (CC, No, Date): US 562162 000502

DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: G06F-001/00

ABSTRACT WORD COUNT: 107

NOTE:

Figure number on first page: 3

LANGUAGE (Publication,Procedural,Application): English; English; English

TEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200150	777
SPEC A	(English)	200150	15547
Total word count - document A			16324
Total word count - document B			0
Total word count - documents A + B			16324

...SPECIFICATION PFX can be independently protected from exposure during transmission by one of two privacy modes:

1. Public-key privacy mode, in which the data is encrypted with the public key of the receiver and the data can be decrypted at the receiver with the corresponding private key; and

2. Password-based privacy mode, in which the data is encrypted with a shared secret key (symmetric key) derived from an input password and the data can be decrypted with the same key at the receiver.

Alternatively, the data may be left unprotected, i.e. no encryption.

The PFX is itself protected from data tampering by one of...

...the receiver; and

2. Password-based integrity mode, in which a message authentication

code is produced by digesting the entire PFX with the HMAC-SHA1 message digest algorithm. The HMAC key is derived from an input password. At the receiver, the digest is re-generated using the same input password and compared against the attached digest. If the...

14/3,K/5 (Item 5 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00985625

System and method for secure data transmission
Vorrichtung und Verfahren zur gesicherten Datenubertragung
Procede et dispositif de transmission securisee de donnees

REFERENCE:

WELLS INC., (244957), World Headquarters, One Elmcroft Road,
Connecticut 06926-0700, (US), (applicant designated states:
AT;BE;CH;CY;DE;DK;ES;FI;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT;SE)

INVENTOR:

Daniels, Edward P., Jr., 75 Magnolia Road, Trumbull, Connect. 0661, (US)

LEGAL REPRESENTATIVE:

Avery, Stephen John et al (47695), Hoffmann Eitle, Patent- und
Rechtsanwalte, Arabellastrasse 4, 81925 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 892519 A2 990120 (Basic)

APPLICATION (CC, No, Date): EP 98113398 980717;

PRIORITY (CC, No, Date): US 895877 970717

DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI;
LU; MC; NL; PT; SE

INTERNATIONAL PATENT CLASS: H04L-009/08;

ABSTRACT WORD COUNT: 128

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9903	889
SPEC A	(English)	9903	3079
Total word count - document A			3968
Total word count - document B			0
Total word count - documents A + B			3968

...SPECIFICATION The term symmetric reflects the fact that both users must have identical keys.

In more technical terms, a symmetric cryptosystem comprises an encryption function, a decryption function, and a shared secret key. The key is a unique string of data bits to which the functions are applied. Two examples of the encipherment/decipherment functions are the National Bureau of Standards Dating Encryption Standard (DES) and the more recent Fast Encipherment Algorithm (FEAL). To transmit a message in privacy, the sender computes "cipher text," which is a function of the encryption function along with the shared secret key and the message to be transmitted. Upon receipt of the cipher text, the recipient computes a transmitted message, which is a function of the decryption function along with the cipher text and the shared secret key, to recover the message. An eavesdropper, who copies the cipher text, but does not know the shared secret key, will find it practically impossible to recover the message. Typically, all details of the enciphering and deciphering functions are well known, and the security of the systems depend solely on maintaining the secrecy of the shared secret key. Conventional symmetric cryptosystems are fairly efficient and can be used for encryption at fairly high data rates, especially if appropriate hardware implementations are used.

Another...

14/3,K/6 (Item 6 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

CYCLOTOMIC POLYNOMIAL CONSTRUCTION OF DISCRETE LOGARITHM CRYPTOSYSTEMS OVER
FINITE FIELDS

AUFBAU EINES ZYKLOTOMISCHEN POLYNOMS EINES KRYPTOSYSTEMS BASIEREND AUF DEM
DISKRETEN LOGARITHMUS UBER ENDLICHE KORPER

CONSTRUCTION POLYNOMIALE CYCLOTOMIQUE DE SYSTEMES CRYPTOGRAPHIQUES A
LOGARITHME DISCRET SUR DES CORPS FINIS

PATENT ASSIGNEE:

AT&T Corp., (1570360), 399 Park Avenue, New York, New York 10043,

(US), (Proprietor designated states: all)

INVENTOR:

Vanstraelen, Arjen, K., 114 West Oak Street, Basking Ridge, NJ 07920, (US)

LEGAL REPRESENTATIVE:

VOSSIUS & PARTNER (100314), Siebertstrasse 4, 81675 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 963635 A1 991215 (Basic)

EP 963635 B1 030730

WO 98036526 980820

APPLICATION (CC, No, Date): EP 97945298 970926; WO 97US17304 970926

PRIORITY (CC, No, Date): US 800669 970214

DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU;

MC; NL; PT; SE

INTERNATIONAL PATENT CLASS: H04L-009/30

NOTE:

No A-document published by EPO

LANGUAGE (Publication, Procedural, Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200331	1224
CLAIMS B	(German)	200331	1224
CLAIMS B	(French)	200331	1348
SPEC B	(English)	200331	9115

Total word count - document A 0

Total word count - document B 12911

Total word count - documents A + B 12911

...SPECIFICATION the order of the subgroup being the second prime number,
selects an integer, receives an intermediate value which is based on the
generator, forms the **shared key** as a function of the intermediate
value and the integer, and **encrypts** the message using the **shared key**

A method for secure communication of a message receives an encrypted
message which has been **encrypted** using a **shared key** formed as a
function of an intermediate value and a selected integer, the
intermediate value being based on a generator of a subgroup of a
multiplicative group of a...

...of the subgroup being a second prime number which is a factor of a
cyclotomic polynomial evaluated at a first prime number, and decrypts the
encrypted message using the **shared key**.

A method for secure communication of a message selects a first prime
number, obtains a cyclotomic polynomial evaluated at the first prime
number, obtains a...

14/3,K/7 (Item 7 from file: 348)

DIALOG(R) File 348:EUROPEAN PATENTS

(c) 2004 European Patent Office. All rts. reserv.

00543502

A cryptosystem for cellular telephony

Geheimubertragungssystem fur zellulare Telefonie

Systeme cryptographique pour telephonie cellulaire

PATENT ASSIGNEE:

AT&T Corp., (589370), 32 Avenue of the Americas, New York, NY 10013-2412,

(US), (Proprietor designated states: all)

INVENTOR:

Reeds III, James Alexander, 127 Southgate Road, New Providence, New

Jersey 07974, (US)

LEGAL REPRESENTATIVE:

Buckley, Christopher Sim Thirsk et al (28912), Lucent Technologies (UK)
Ltd, 5 Mornington Road, Woodford Green, Essex IG8 0TU, (GB)
PATENT (CC, No, Kind, Date): EP 532228 A2 930317 (Basic)
EP 532228 A3 940413
EP 532228 B1 991215
APPLICATION (CC, No, Date): EP 92308000 920903;
PRIORITY (CC, No, Date): US 759309 910913
DESIGNATED STATES: DE; FR; GB; SE
INTERNATIONAL PATENT CLASS: H04L-009/32; H04L-009/06
ABSTRACT WORD COUNT: 83
NOTE:

Figure number on first page: 2

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9950	1538
CLAIMS B	(German)	9950	1409
CLAIMS B	(French)	9950	1601
SPEC B	(English)	9950	5329
Total word count - document A			0
Total word count - document B			9877
Total word count - documents A + B			9877

...SPECIFICATION inverting, symmetric key cryptosystem may comprise three stages. The first stage is an autokeyed encryption on the plaintext. The second stage is a self-inverting cipher where the encryption key is derived from a portion of the message as encrypted by the first stage. The third stage is a second autokeyed decryption that corresponds to the autokeyed encryption of the first stage.

Brief...

...radio providers interconnected for service to both stationary and mobile telephones and the like;

FIG.2 depicts the process for directing the creation of a shared secret data field and the verification of same;

FIG.3 shows the elements that are concatenated and hashed to create the shared secret data ;

FIG.4 shows the elements that are concatenated and hashed to create the verification sequence;

FIG.5 shows the elements that are concatenated and hashed...

14/3,K/8 (Item 8 from file: 348)

File 348:EUROPEAN PATENTS

European Patent Office. All rts. reserv.

216587

Decoding transmitted scrambled signals.

Dekodierung ubertragener verschleierter Signale.

Decodage de signaux transmis brouilles.

PATENT ASSIGNEE:

PHILIPS ELECTRONICS UK LIMITED, (215201), Philips House 1-19 Torrington Place, London WC1E 7HD, (GB), (applicant designated states: GB)

N.V. Philips' Gloeilampenfabrieken, (200769), Groenewoudseweg 1, NL-5621

BA Eindhoven, (NL), (applicant designated states: DE;FR;IT;SE)

INVENTOR:

Growth, Gerald Offley, c/o Mullard Mitcham 2 New Road, Mitcham Surrey CR4 4XY, (GB)

Brennand, Peter Robert, c/o Mullard Mitcham 2 New Road, Mitcham Surrey CR4 4XY, (GB)

LEGAL REPRESENTATIVE:

Andrews, Arthur Stanley et al (27711), PHILIPS ELECTRONICS Patents and Trade Marks Department Philips House 1-19 Torrington Place, London WC1E 7HD, (GB)

PATENT (CC, No, Kind, Date): EP 256596 A2 880224 (Basic)
EP 256596 A3 900321
EP 256596 B1 940302

APPLICATION (CC, No, Date): EP 87201500 870806;
PRIORITY (CC, No, Date): GB 8619737 860813; GB 8625487 861024
DESIGNATED STATES: DE; FR; GB; IT; SE
INTERNATIONAL PATENT CLASS: H04N-007/167;
ABSTRACT WORD COUNT: 156

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPBBF1	753
CLAIMS B	(German)	EPBBF1	671
CLAIMS B	(French)	EPBBF1	799
SPEC B	(English)	EPBBF1	6069
Total word count - document A			0
Total word count - document B			8292
Total word count - documents A + B			8292

...SPECIFICATION documents refer to a system, known as System B, which is a shared key over-air addressing system where the scrambling process i.e. the **process that** renders the picture and/or sound/data unintelligible, is derived from a truly random control word (CW1 or CW2). The control word and any programme...

...sent over-air in an Entitlement Checking Message (ECM). The Supplementary key(s) together with customer messages or authorisations (M) are further encrypted using a **shared** distribution **key** (D) and the resulting cryptogram D(M,S) is sent **over -air an** Entitlement Management Message (EMM). The **shared** distribution **key** is stored within the viewer's conditional **access** sub-system (**CASS**) which **enables** this sub-system to **derive** the Control Word or words, and to store any authorisations. The EMM has two data streams of which the Unique Customer packets are used to update the CASS in terms of **shared** distribution **key** , address, etc. and the Shared Customer packets contain the actual **entitlements** or **authorisations** .

The above System B proposal is designed to operate at any one time in one mode, either a subscription mode or a pay-per-view...

14/3,K/9 (Item 1 from file: 349)
FILE 349:PCT FULLTEXT
WIPO/Univentio. All rts. reserv.

01066457 **Image available**

SECURE MOBILE AD-HOC NETWORK AND RELATED METHODS
RESEAU AD HOC MOBILE SECURISE ET PROCEDES ASSOCIES

Patent Applicant/Assignee:

HARRIS CORPORATION, 1025 W. Nasa Blvd., Melbourne, FL 32919, US, US
(Residence), US (Nationality)

Inventor(s):

BILLHARTZ Thomas Jay, 2355 Polonius Lane, Melbourne, FL 32934, US,
FLEMING Frank Joseph, 601 Morning Cove Circle, Palm Bay, FL 32909, US,

Legal Representative:

YATSKO Michael S (et al) (agent), Harris Corporation, 1025 W. Nasa Blvd,
Melbourne, FL 32919, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200396606 A1 20031120 (WO 0396606)
Application: WO 2003US14322 20030507 (PCT/WO US0314322)
Priority Application: US 2002143145 20020510

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU
CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP
KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO
RU SD SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE
SI SK TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

AF GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW

FA AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 4654

Fulltext Availability:
Detailed Description

Detailed Description

... used to produce the same value output from the algorithm without access to the original input, including the secret key. Thus, by using a secret **key encrypted** with a one-way **function** to, in turn, encrypt plain **text** to be sent in wireless ad-hoc network messages, the secret key becomes much less vulnerable to attacks such as the Fluhrer attack.

In accordance...
...security function is enabled the encrypted messages include cipher text and an initialization vector (IV). The IV is normally used in WEP to augment the **shared** secret **key** used by the wireless stations and access points and produce a different key sequence for each packet of text, thus avoiding two **cipher** texts having the same **key** stream.

As noted above, even the use of the IV called for in the 802.11 standard does not make WEP immune to attacks such...

14/3,K/10 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

Image available

SYSTEM AND METHOD FOR SECURING A COMMUNICATION CHANNEL SYSTEME ET PROCEDE PERMETTANT DE SECURISER UN CANAL DE COMMUNICATION

Patent Applicant/Assignee:

WAVE7 OPTICS INC, 1075 Windward Ridge Parkway, Suite 170, Alpharetta, GA 30005, US, US (Residence), US (Nationality)

Inventor(s):

THOMAS Stephen A, 4397 Windsor Oaks Circle, Marietta, GA 30350, US,
BERSON Thomas A, 764 Forest Avenue, Palo Alto, CA 94301, US,
ANTHONY Deven J, 330 Oakridge Terrace, Alpharetta, GA 30005, US,
GONG Guang, 412 Woodrow Drive, Waterloo, Ontario N2T 2V7, CA,
FARMER James O, 3602 Preston Court, Lilburn, GA 30047, US,

Legal Representative:

WIGMORE Steven P (agent), King & Spalding, 191 Peachtree Street, Atlanta, GA 30303-1763, US,

Parent and Priority Information (Country, Number, Date):

Patent: WO 200323980 A2-A3 20030320 (WO 0323980)

Application: WO 2002US28734 20020910 (PCT/WO US0228734)

Priority Application: US 2001318447 20010910; US 2002388497 20020614

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU

CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP

KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO

RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW

(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 19010

Fulltext Availability:
Detailed Description

Detailed Description

... aspect of the present invention, a method for authenticating and exchanging parameters between two parties over an unsecured data channel

for deriving a shared secret **encryption key** can provide perfect forward secrecy using a minimum amount of communications bandwidth.

That is, the method for authenticating and exchanging parameters for **deriving a shared encryption key** can prevent unauthorized access to **encrypted messages** even if a party later divulges its private key. The method can employ an asymmetric **encryption** algorithm, such as a public-**key** algorithm, that functions as a carrier to transport the parameters of a symmetric algorithm such as key exchange parameters of the Diffie-Hellman protocol.

If the second party is valid. If the public key certificate is valid, the first party can send to the second party a message comprising an **encrypted non-secret key** exchange value and a random number, where the value and the random number are encrypted with the public key belonging to the second party...with other exclusive "or" operations from other shift registers in a group of shift registers.

In the method for authenticating and exchanging parameters, a public **key encryption** algorithm can function as a carrier to transport the parameters of a key exchange protocol. By operating in this manner, the method can reduce the number of messages needed to authenticate and exchange the parameters for **deriving a shared secret key** compared to the number of **messages** used in the conventional art.

Illustrative Operating Environment for the Invention
Referring now to the drawings, in which like numerals represent like elements throughout the...1145 can further comprise the subscriber optical interface's 140 non-secret key exchange parameter 1140 and the nonce 1150. The nonce 1150 can be **encrypted** with the **shared encryption key**. In response to the third message C, the laser transceiver node 120 can take the subscriber optical interface's 140 non-secret key exchange parameter 1140 and its first secret key parameter such as small letter x to **derive** the **shared encryption key**.

The three **messages** described above (**messages** A, B, C combine public key

cryptology and a key exchange protocol to take advantage of the benefits of both types of key distribution. Specifically...

...a carrier to transport the parameters of a key exchange protocol to verify the identity of the subscriber optical interface 140, to establish a symmetrical **key** to use for data **encryption**, and to provide perfect forward secrecy.

In order to agree on a secret key, the Diffie-Hellman key exchange protocol is used, as described below...

14/3,K/11 (Item 3 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00820782 **Image available**

A SECURE COMMUNICATION METHOD FOR MOBILE IP
PROCEDE DE COMMUNICATION SECURISE POUR IP MOBILE
Patent Applicant/Assignee:

TELEFONAKTIEBOLAGET LM ERICSSON (publ), S-126 25 Stockholm, SE, SE
(Residence), SE (Nationality)

Inventor(s):

AHONEN Pasi, Salotie 5, FIN-90630 Oulu, FI,

Legal Representative:

LUNDHOLM-CARLSSON Lena (agent), Ericsson Radio Systems AB, Patent Unit
Research, S-164 80 Stockholm, SE,

Priority Information (Country, Number, Date):

WO 200154379 A1 20010726 (WO 0154379)
WO 2001SE49 20010112 (PCT/WO SE0100049)

Priority Application: GB 000961 20000118

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ
DE DK DM DZ EE ES FI GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC
LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI
SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
AF BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
AG AH GM KE LS MW MZ SD SL SZ TZ UG ZW
EA AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 7481

Fulltext Availability:

Detailed Description

Detailed Description

... above, the authentication method for the exchange has already been negotiated (during IKE negotiation) from four different types of candidates.

- digital signature,
- authentication with public key encryption (two different),
- pre-shared key .

Now, the selected authentication method will be applied in this authentication exchange, and the result will be three groups of authenticated keying material (keymat).

- the keymat used by the ISAKW SA to protect the confidentiality of its messages,
- the keymat used by the ISAKMP SA to authenticate its messages ,
- the keymat used to derive keys for non-ISAKMP security associations.

This keying material is proven to be authentic, because both the Initiator and

14/3,K/12 (Item 4 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2004 WIPO/Univentio. All rts. reserv.

00785490 **Image available**

INTERNET PROTOCOL MOBILITY ARCHITECTURE FRAMEWORK

CADRE D'ARCHITECTURE DE MOBILITE PAR PROTOCOLE INTERNET

Patent Applicant/Assignee:

NORTEL NETWORKS LIMITED, World Trade Center of Montreal, 8th floor, 380
St. Antoine Street West, Montreal, Quebec H2Y 3Y4, CA, CA (Residence),
CA (Nationality)

Inventor(s):

AKHTAR Haseeb, 3102 Pamela Place, Garland, TX 75044, US,
QADDOURA Emad A, 1320 Wateredge Drive, Plano, TX 75093, US,
BECKER Carey B, 1529 Faringdon Drive, Plano, TX 75075, US,
PATIL Basavaraj B, 7616 Capella Court, Plano, TX 75025, US,
BARNES March H, 3820 Hidden Trail, Flower Mound, TX 75028, US,
WURCH Donald L, 3607 Highpoint Drive, Rockwall, TX 75078, US,
COFFIN Russell C, 5608 Crowndale Drive, Plano, TX 75093-8500, US,
ZHU Zemin, 3808 Neiman Road, Plano, TX 75025, US,
TUMMALA Rambabu, 4324 Giovanni, Plano, TX 75024, US,
NARAYANAN Raja, 1100 Meredith Lane #728, Plano, TX 75093, US,
Mohamed, 118 Briar Oaks Street, Murphy, TX 75095, US,
Q, 1605 Meadowgate Drive, Richardson, TX 75081, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200119050 A2-A3 20010315 (WO 0119050)

Application: WO 2000IB1553 20000908 (PCT/WO IB0001553)

Priority Application: US 99152916 19990908; US 99156669 19990929; US
99157289 19991001; US 99157449 19991004; US 2000192411 20000327; US
2000657516 20000907

Designated States: AE AL AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE
EG FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT
LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT
UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 85222

Fulltext Availability:

Detailed Description

Detailed Description

FIG. 14 presents an integrated AAA interface (through a single IP address) to the rest of the IP Network 108 and is configured for forwarding AAA messages to the appropriate function.

within the NSF 104 (FIGS. 4A, 4B, 4E, and 4F) responsible for a particular function. This allows an operator specific internal architecture of an NSF...function 462 or the mobility manager SMM 464j, performs an AAA function,, that entity generates an AAA message and sends it to a "local" AAA function. The "local" AAA function is defined with respect to FIG. 12 as the AAA function 462A, 462B, or 450C located at the LSF 106A, 106B...

14/3,K/13 (Item 5 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2004 WIPO/Univentio. All rts. reserv.

00736410 **Image available**

DATA AUTHENTICATION SYSTEM EMPLOYING ENCRYPTED INTEGRITY BLOCKS
SYSTEME D'AUTHENTIFICATION DE DONNEES A BLOCS D'INTEGRITE CRYPTES

Patent Applicant/Assignee:

ARM MICROSYSTEMS INC, M/S PALL-521, 901 San Antonio, Palo Alto, CA 94303,
US (Residence), US (Nationality)

Inventors:

ARMAN Radia Joy, 10 Huckleberry Lane, Acton, MA 01720, US

HANNA Stephen R, 3 Beverly Road, Bedford, MA 01730, US

Legal Representative:

SHEEHAN Patricia A, Cesari and McKenna, LLP, 30 Rowes Wharf, Boston, MA
02110, US

Patent and Priority Information (Country, Number, Date):

Patent: WO 200049764 A1 20000824 (WO 0049764)

Application: WO 2000US3960 20000216 (PCT/WO US0003960)

Priority Application: US 99250935 19990218

Designated States: AE AL AU BA BB BG BR CA CN CR CU CZ DM EE GD GE HR HU ID
IL IN IS JP KP KR LC LK LR LT LV MA MG MK MN MX NO NZ PL RO SG SI SK TR
TT UA UZ VN YU ZA

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE

(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG

(AP) GH GM KE LS MW SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 7157

Fulltext Availability:

Detailed Description

Detailed Description

... a secret key is commonly referred to as a message integrity code, or

"MIC," process. The MIC process produces an integrity code by concatenating the **shared secret key** with the data and then encoding the data and the **key** using a cryptographic hash **function**. The result, which is the integrity **code**, is then sent along with the data to a recipient who shares the secret key. The recipient similarly concatenates the **shared secret key** with the received data and encodes the data and the **key** using the hash **function**. If the result matches the received **integrity code**, the data is considered authentic. The MIC communication process works well and is relatively reliable, assuming the holders of the **shared key** are trusted. However, this process still requires producing a hash based on all of the data bytes in the data packet, and is thus still...

...data authentication system that at the sender produces for a plurality of data packets a plurality of "integrity checks" that it then encrypts with a **shared secret key** and sends as an "integrity block." A recipient decrypts the integrity block using the **shared secret key** and reproduces the integrity checks. It then uses the integrity checks to authenticate the associated data packets. As discussed below, the authentication system uses a...

14/3,K/14 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00732010 **Image available**

METHODS FOR OPERATING INFRASTRUCTURE AND APPLICATIONS FOR CRYPTOGRAPHICALLY-SUPPORTED SERVICES
PROCEDES D'EXPLOITATION D'UNE INFRASTRUCTURE ET APPLICATIONS POUR SERVICES BASES SUR LA CRYPTOGRAPHIE

Patent Applicant/Inventor:

MONTGOMERY Charles T, Suite 22, 55 Broad Street, New York, NY 10004, US,
US (Residence), US (Nationality), (Designated only for: US)
MONTGOMERY Stuart, Suite 22, 55 Broad Street, New York, NY 10004, US, US
(Residence), US (Nationality), (Designated only for: US)
MONTGOMERY Marcel Mordechay, Suite 22, 55 Broad Street, New York, NY 10004, US,
US (Residence), US (Nationality), (Designated only for: US)

Legal Representative:

LAZAR Dale S, Pillsbury Madison & Sutro, LLP, 1100 New York Avenue, N.W.,
Washington, DC 20005, US

Patent and Priority Information (Country, Number, Date):

Patent: WO 200045347 A1 20000803 (WO 0045347)
Application: WO 2000US2012 20000128 (PCT/WO US0002012)
Priority Application: US 99117752 19990128; US 2000492534 20000127

Designated States: AU CA JP US

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE

Publication Language: English

Filing Language: English

Fulltext Word Count: 13340

Fulltext Availability:

Detailed Description

Detailed Description

... asymmetric techniques are available, as well as access-control technology.

Furthermore, in communication it is assumed that each message that needs to be secured is **encrypted** by a **key**. The **key** is either shared by the sender and the receiver or derived from a key exchange protocol (for example, the Diffie-Hellman key exchange where one or both parties utilize a public **key** and the parties can **derive** a **shared key**). Further, **messages** that need to be signed for authenticity and proof of origin, are signed by the sender. **Shared** cryptographic **information** may be used for binding and connecting messages, logging and monitoring of messages.

Within a context of message exchange (a transaction), messages may be
received...

14/3,K/15 (Item 7 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00483529

CRYPTOGRAPHIC CO-PROCESSOR
COPROCESSEUR CRYPTOGRAPHIQUE

Patent Applicant/Assignee:

INFORMATION RESOURCE ENGINEERING INC,
KAPLAN Michael M,
DOUD Robert Walker,
KAVSAN Bronislav,
OBER Timothy,
REED Peter,

Inventor(s):

KAPLAN Michael M,
DOUD Robert Walker,
KAVSAN Bronislav,
OBER Timothy,
REED Peter,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9914881 A2 19990325

Application: WO 98US19316 19980916 (PCT/WO US9819316)

Priority Application: US 9759082 19970916; US 9759839 19970916; US
9759840 19970916; US 9759841 19970916; US 9759842 19970916; US 9759843
19970916; US 9759844 19970916; US 9759845 19970916; US 9759846 19970916
; US 9759847 19970916

Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES
FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD
MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US
UZ VN YU ZW GH GM KE LS MW SD SZ UG SG AM AZ BY KG KZ MD RU TJ TM AT BE
CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN
GW ML MR NE SN TD TG

Publication Language: English

Fulltext Word Count: 95649

Fulltext Availability:

Detailed Description

Detailed Description

... only accessible to the internal function blocks and the Security
Kernel. Included in these Laser Variable bits are.

- * 1 12-bit Local Storage Variable (Master Key - Encryption - Key)

- 0 80-bit Randomizer Seed

- * 48-bits Program Control Data (Enables/Disables various IC features and
configures
the IC)

- * 16-bit CRC of the Laser Data

The Program Control Data (PCD) bits include configuration for permitted
Key

lengths, Algorithm Enables, Red KEK loading, Internal IC Pulse Shaping
Characteristics, etc. Some of the PCD settings may be overridden with a
Digitally Signed Token...

...C when it boots. These Tokens are created by IRE and each is targeted to
a specific CryptIC using a Hash of its unique identity (**derived** from
the above Laser Variable).

Downloadable Secure Code

The CryptIC is designed to allow additional Security Functions to be
added to the device through a Secure Download feature. Up to 16k words...

...be given the security privileges of the Kernel firmware. All downloaded

19/3,K/1 (Item 1 from File: 348)
PUBLICATION File 348:EUROPEAN PATENTS
2004 European Patent Office. All rts. reserv.

01667262

Electronic value data communication method and system between IC cards
Verfahren und System zur elektronischen Wertdatenkommunikation zwischen
Chipkarten

Methode et systeme de communication de donnees electroniques de valeur
entre cartes a puce

PATENT ASSIGNEE:

NTT DoCoMo, Inc., (3031180), 11-1, Nagatacho 2-chome, Chiyoda-ku, Tokyo
100-6150, (JP), (Applicant designated States: all)
Sakamura, Ken, (4438300), 4-9-2 Osaki, Shinagawa-ku, Tokyo 141-0032, (JP)
, (Applicant designated States: all)
Koshizuka, Noboru, (4438320), 2-27-20, Nishikubo, Musashino-shi, Tokyo
180-0013, (JP), (Applicant designated States: all)

INVENTOR:

Ishii, Kazuhiko, Intellectual Property Department, NTT DoCoMo, Inc.,
Sanno Park Tower, 11-1, Nagata-, cho 2-chome, Chiyoda-ku, Tokyo
100-6150, (JP)
Mori, Kensaku, Intellectual Property Department, NTT DoCoMo, Inc., Sanno
Park Tower, 11-1, Nagata-, cho 2-chome, Chiyoda-ku, Tokyo 100-6150,
(JP)
Aono, Hiroshi, Intellectual Property Department, NTT DoCoMo, Inc., Sanno
Park Tower, 11-1, Nagata-, cho 2-chome, Chiyoda-ku, Tokyo 100-6150,
(JP)
Hongo, Sadayuki, Intellectual Property Department, NTT DoCoMo, Inc.,
Sanno Park Tower, 11-1, Nagata-, cho 2-chome, Chiyoda-ku, Tokyo
100-6150, (JP)
Sakamura, Ken, Intellectual Property Department, NTT DoCoMo, Inc., Sanno
Park Tower, 11-1, Nagata-, cho 2-chome, Chiyoda-ku, Tokyo 100-6150,
(JP)
Koshizuka, Noboru, Intellectual Property Dept., NTT DoCoMo, Inc., Sanno
Park Tower, 11-1, Nagata-, cho 2-chome, Chiyoda-ku, Tokyo 100-6150,
(JP)

LEGAL REPRESENTATIVE:

Bockhorni, Josef et al (46049), Patent-& Rechtsanwalte, Grosse,
Bockhorni, Schumacher, Forstenrieder Allee 59, 81476 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 1369829 A2 031210 (Basic)
EP 1369829 A3 040204

APPLICATION (CC, No, Date): EP 2003012737 030604;

PRIORITY (CC, No, Date): JP 2002164808 020605

DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR;
HU; IE; IT; LI; LU; MC; NL; PT; RO; SE; SI; SK; TR

EXTENDED DESIGNATED STATES: AL; LT; LV; MK

INTERNATIONAL PATENT CLASS: G07F-007/10

ABSTRACT WORD COUNT: 97

NOTE:

Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200350	574
SPEC A	(English)	200350	4150
Total word count - document A			4724
Total word count - document B			0
Total word count - documents A + B			4724

...SPECIFICATION B sends the MAC generated in the preceding step of (10),
to A (message (square) in Fig. 4).

(12) A performs a calculation of the **message authentication code**
generating **function** with the common **key** **k(underscore))AB** and the
messages (square), (square), and (square). The result should be equal to
the MAC having been sent in the preceding step of (11). When they are
equal...

...k(underscore)AB proves that the other party knows the random number A and the random number B.
 3) Since the random number A was **encrypted** with the public key B and then transmitted, only B knows this except for itself (A).
 4) It is, therefore, proved that the other party in communication is B
 ...

...correspondent proved to be B also knows the messages (square), (square), and (square). Therefore, the messages exchanged heretofore are definitely those from B and the **messages** having been **transmitted** must also correctly be delivered to B.

(13) A confirms from the preceding step (12) that the correspondent is B and the **messages** heretofore were correctly **transmitted** and **received** to and from B.

(14) A performs a calculation of the **message authentication code** generating **function** with the common **key** k(underscore)AB and the **messages** (square), (square), (square), and (square) to generate a MAC. MAC is a code (numerical number) authenticating that the messages were correctly transmitted and received.

{15...

19/3,K/2 (Item 2 from file: 348)
 DIALOG(R)File 348:EUROPEAN PATENTS
 (c) 2004 European Patent Office. All rts. reserv.

01648393

Secure communication via the internet
 Sichere Kommunikation uber Internet
 Communication securisee via l'Internet
 PATENT ASSIGNEE:

Izecom B.V., (4085830), Brantasgracht 10, 1019 RK Amsterdam, (NL),
 (Applicant designated States: all)

INVENTOR:

Forman, Christine, Brantasgracht 10, 1019 RK Amsterdam, (NL)

LEGAL REPRESENTATIVE:

Hoekstra, Jelle (89252), DeltaPatents, Twinning Center Eindhoven, De
 Zaaile 11, Postbus 80, 5600 AB Eindhoven, (NL)

PATENT (CC, No, Kind, Date): EP 1357697 A1 031029 (Basic)

APPLICATION (CC, No, Date): EP 2002079287 021017;

PRIORITY (CC, No, Date): EP 200276498 020416

DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR;

IE; IT; LI; LU; MC; NL; PT; SE; SK; TR

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: H04L-009/30

ABSTRACT WORD COUNT: 152

NOTE:

Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200344	1078
SPEC A	(English)	200344	7244
Total word count - document A			8322
Total word count - document B			0
Total word count - documents A + B			8322

...SPECIFICATION out-of-date keys), need not to inform other users where to download software from and how to use the software to create and store keys .

As defined in the **dependent** claim 2, the **communication** of the **message** takes place via a server. In this way, the sending client only needs to have access to the public key of the secure server. This simplifies checking whether the key is still valid. Moreover, the sending client is relieved from having to manage the **email** in the situation that the **receiving** client has not yet obtained a key pair. Preferably, the sending client always uses the services of the secure

...for delivery of secured content. Alternatively, the sending client may send the email directly to the receiving client encrypted with the public key of the receiving client if this key is available in the key server. If the client sends directly, the secure server is used if no...

19/3,K/3 (Item 3 from file: 348)
DIALOG(R) File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01507203

Devices and processes for the transmission and implementation of control instructions for access to functionalities of receivers
Vorrichtungen und Verfahren zur Übertragung und Implementierung von Steuerungsanweisungen zum Zugriff auf Empfängerfunktionalitäten
Dispositifs et procedes pour la transmission et la mise en oeuvre d'instructions de controle pour acceder a des fonctionnalites de recepteurs

PATENT ASSIGNEE:

Thomson Licensing S.A., (2880641), 46, quai A.Le Gallo, 92100
Boulogne-Billancourt, (FR), (Applicant designated States: all)

INVENTOR:

Lesenne, Laurent, 26 rue des Tertres, 5690 Acigne, (FR)
Pasquier, Frederic, 26 rue d'Ouessant, 5890 Laille, (FR)

LEGAL REPRESENTATIVE:

Kubler, Thierry (93483), Thomson multimedia, 46, Quai Alphonse Le Gallo,
Boulogne Billancourt cedex, (FR)

(CC, No, Kind, Date): EP 1261166 A2 021127 (Basic)
EP 1261166 A3 030326

APPLICATION (CC, No, Date): EP 2002011040 020517;

PRIORITY (CC, No, Date): FR 016771 010523

DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI;
LU; MC; NL; PT; SE; TR

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: H04L-029/06; H04L-012/18; H04N-007/16;

H04N-005/00; H04N-007/088; H04N-007/173

ABSTRACT WORD COUNT: 126

NOTE:

Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200248	920
SPEC A	(English)	200248	7389
Total word count - document A			8309
Total word count - document B			0
Total word count - documents A + B			8309

...SPECIFICATION keys K1)), K2)) ... Kn)) of the enciphering library 15.

The identification module 27 is designed to perform the identification according to one of the identification keys K'i)), as a function of instructions given by the message identification device 4. Moreover, the latter comprises:

- an identification control unit 21, capable of triggering the identification module 27 by communicating the necessary information thereto...

...unit 23 for extracting from the message MSG the key identifier KeyID, giving the current identification key K'i)) chosen in correspondence with the current enciphering key K'i)) of the sender 2.

The succinct account given above is essentially functional, and it is exclusively centred around specific features in conjunction with a particular assembly for securing and identifying messages. The sender 1 can in reality comprise several securing devices such as that referenced 15, possibly in combination. For example, the securing of the messages combines encryption...

19/3,K/4 (Item 4 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01300642

Secure data transmission over a client-server network
Sichere Datenübertragung über ein Client-Server Netzwerk
Transmission securisée de données sur un réseau du type client-serveur
PATENT ASSIGNEE:

Kizna Corporation, (3153331), 1209 Orange St., Wilmington, Delaware 19801
, (US), (Applicant designated States: all)

INVENTOR:

Miyazawa, Takeo, Prestige S&T W2, 12-3 Shimo-Renjaku 4-chome, Mitaka-shi,
Tokyo 181-0013, (JP)
Okada, Tetsuya, Tokyu-Heim, 6-5 Koenji-Minami 3-chome, Suginami-ku, Tokyo
166-0003, (JP)

LEGAL REPRESENTATIVE:

Brown, Kenneth Richard et al (28831), R.G.C. Jenkins & Co. 26 Caxton
Street, London SW1H 0RJ, (GB)

PATENT (CC, No, Kind, Date): EP 1115049 A2 010711 (Basic)
EP 1115049 A3 021030

APPLICATION (CC, No, Date): EP 2000310849 001206;

PRIORITY (CC, No, Date): JP 99348133 991207

DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI;
LU; MC; NL; PT; SE; TR

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: G06F-001/00; H04L-029/06

ABSTRACT WORD COUNT: 77

NOTE:

Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200128	1018
SPEC A	(English)	200128	6135
Total word count - document A			7153
Total word count - document B			0
Total word count - documents A + B			7153

...SPECIFICATION a predetermined safe protocol such as SSL (Secure Sockets Layer). In SSL, the server and the client exchange a security policy and set a selected **encryption key**. At this time the server and the client exchange a random number. Then the server sends an electronic certificate to the client, which the client...

...the server. Then three random numbers, including the two random numbers exchanged first between both ends of the communication, are compressed using such a hash **function** as MD5, and a common **key** for **encrypting** a **message** and a **message** authentication code for preventing alteration are generated. Hereafter, communication is performed while data is **encrypted** by a common **key** method. The hash function is an operation method to generate a pseudo-random number based on input data, and input data cannot be reproduced from...

...Secure Hypertext Transfer Protocol) is known as a similar protocol.

According to a conventional security method, it is possible to increase the security of a **message exchange** between a server and a client and to prevent a third party from intercepting and reading a message to a degree. But the security of...

19/3,K/5 (Item 5 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00761395

USER AUTHENTICATION IN A COMMUNICATIONS NETWORK
BENUTZERAUTHENTIFIZIERUNG IN EINEM KOMMUNIKATIONSNETZ
AUTHENTIFICATION DES UTILISATEURS DANS UN RESEAU DE COMMUNICATION

APPLICANT:

BRITISH TELECOMMUNICATIONS public limited company, (846100), 81 Newgate
Street, London EC1A 7AJ, (GB), (Proprietor designated states: all)

INVENTOR:

HARDING, Peter, Maxwell, 79 The Seafront, Hayling Island Hants PO10 7HQ,
(GB)

HICKS, Richard, Middleton, 21 Birchwood Drive Rushmere & Andrew, Ipswich
Suffolk IP5 7EB, (GB)

KINGAN, Jonathan, James, 20 Warwick Road, Ipswich Suffolk IP4 2QD, (GB)

MEYERSTEIN, Michael, Victor, 27 Mayfields Martlesham Heath, Ipswich
Suffolk IP5 7TU, (GB)

NOLDE, Keith, Eric, 10 Whitethorn Road, Warren Heath Ipswich IP3 8SS,
(GB)

RABSON, John, Limes Farm House Eyke, Woodbridge Suffolk IP12 2QG, (GB)

RANGER, Jonathan, Crispin, 189 Humber Douly Lane, Ipswich Suffolk IP4 3PD,
(GB)

ROBERTS, David, Anthony, 7 Rowanmayes Close, Ipswich IP2 9SX, (GB)

STIRLAND, Mark, Jonathan, Albert Villa Dockamere, Bramford Ipswich IP1
1UX, (GB)

SWALE, Richard, Paul, 4 Fairbairn Avenue Kesgrave, Ipswich Suffolk IP5
7YS, (GB)

LEGAL REPRESENTATIVE:

Lloyd, Barry George William et al (42974), BT Group Legal Services,
Intellectual Property Department, 8th Floor, Holborn Centre, 120
Holborn, London EC1N 2TE, (GB)

PATENT (CC, No, Kind, Date): EP 779003 A1 970618 (Basic)

EP 779003 B1 991006

WO 9605675 960222

APPLICATION (CC, No, Date): EP 95927903 950816; WO 95GB1937 950816

PRIORITY (CC, No, Date): GB 9416595 940817

DESIGNATED STATES: BE; CH; DE; DK; ES; FR; GB; IT; LI; NL; PT; SE

INTERNATIONAL PATENT CLASS: H04L-009/32; H04Q-003/00

NOTE:

No A-document published by EPO

LANGUAGE (Publication, Procedural, Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9940	1128
CLAIMS B	(German)	9940	1022
CLAIMS B	(French)	9940	1308
SPEC B	(English)	9940	5634
Total word count - document A			0
Total word count - document B			9092
Total word count - documents A + B			9092

...SPECIFICATION or each first key being loaded into the network
termination unit for later use with the first algorithm in authenticating
a line. Advantageously, the first **key** may be a **function** of the
identification **code encrypted** by the second **key** using the security
algorithm.

In a preferred embodiment, the transaction number is a variable number
which is changed after each authentication attempt.

The security node...

...Conveniently, the security node may prevent access to the network for
the network termination unit in the event that no match between the
expected and **received authentication codes** is made within a
predetermined duration.

Preferably, the network termination unit transmits a negative
acknowledgement to the security node in the event that no challenge...

01068436 **Image available**

ENCRYPTION, AUTHENTICATION, AND KEY MANAGEMENT FOR MULTIMEDIA CONTENT
PRE-ENCRYPTION

CHIFFREMENT, AUTHENTIFICATION ET GESTION DE CLES POUR UN PRE-CHIFFREMENT DE
CONTENU MULTIMEDIA

Patent Applicant/Assignee:

GENERAL INSTRUMENT CORPORATION, 101 Tounament Drive, Horsham, PA 19044,
US, US (Residence), US (Nationality)

Inventor(s):

PETERKA Petr, 5126 Caminito Vista Lujo, San Diego, CA 92130, US,
MEDVINSKY Alexander, 8873 Hampe Court, San Diego, CA 92129, US,
CHEN Kuang-Ming, 12110 Wooded Vista Lane, San Diego, CA 92128, US,

Legal Representative:

NICHOLS Steven L (agent), River Park Corporate Center One, 10653 S. River
Front Pkwy., Suite 150, South Jordan, UT 84095, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200398867 A2-A3 20031127 (WO 0398867)

Application: WO 2003US1955 20030122 (PCT/WO US03001955)

Priority Application: US 2002350678 20020122; US 2003349263 20030121

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU

CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP

KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO

RU SL SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW

FI AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT SE SI

UA BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 9111

Fulltext Availability:

Detailed Description

Detailed Description

19/3,K/7 (Item 2 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2004 WIPO/Univentio. All rights reserved.

01066923

SYSTEM AND METHOD OF SECURE AUTHENTICATION AND BILLING FOR GOODS AND
SERVICES USING A CELLULAR TELECOMUNICATION AND AN AUTHORIZATION
INFRASTRUCTURE

SYSTEME ET PROCEDE D'AUTHENTIFICATION ET DE FACTURATION SECURISEES POUR DES
PRODUITS ET DES SERVICES AU MOYEN D'UNE TELECOMMUNICATION CELLULAIRE ET
D'UNE STRUCTURE D'AUTORISATION

Patent Applicant/Assignee:

NOKIA CORPORATION, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence),
FI (Nationality)

NOKIA INC, 6000 Connection Drive, Irving, TX 75039, US, US (Residence),
US (Nationality), (Designated only for: LC)

Inventor(s):

ASOKAN Nadarajah, Ankkurinvärsi 6 K, FIN-02320 Espoo, FI,
GINZBOORG Philip, Ylakaupinkuja 1 B 10, FIN-02360 Espoo, FI,

Legal Representative:

BRUNDIDGE Carl I (agent), Antonelli, Terry, Stout, & Kraus, LLP, Suite
1800, 1300 North Seventeenth Street, Arlington, VA 22209, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200396140 A2 20031120 (WO 0396140)

Application: WO 2003IB1777 20030507 (PCT/WO IB0301777)

Priority Application: US 2002141879 20020510

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU

CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP

KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OA OH PL PT RO
RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE
SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 12859

Fulltext Availability:

Detailed Description

Detailed Description

... FIG. 4, the HLR/AUC I 00 responds with message 230 containing a random number (RAND) 41 0, a signed response (SRES) 450, and an **encryption key** (Kc) 400. The gateway 60 takes the Kc 400 and uses it to compute an integrity key (K) based on the formula $K = f(\{Kc\})$.
... gateway 60 would then store the SID, IMSI, RAND 440, SRES 450 and K in a single record in the gateway's 60 memory. Thereafter, **message** 14 is sent from the gateway 60 to the mobile station 20 and contains RAND 440 and M1. M1 is computed based upon a **message authentication code** (MAC) **function** using integrity **key** (K) And RAND 440. The formula used is represented as $M1 = MAC(K, \{RAND\})$. The purpose of a MAC is to facilitate, without the use...

19/3,K/8 (Item 3 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

© 2004 WIPO/Univentio. All rts. reserv.

Image available

SECURITY DEVICES AND PROCESSES FOR PROTECTING AND IDENTIFYING MESSAGES
DISPOSITIFS ET PROCÉDES DE SÉCURITÉ POUR LA PROTECTION ET L'IDENTIFICATION
DE MESSAGES

Patent Applicant/Assignee:

THOMSON LICENSING S A, 46 Quai Alphonse Le Gallo, F-92100

BOULOGNE-BILLANCOURT, FR, FR (Residence), FR (Nationality), (For all designated states except: US)

Patent Applicant/Inventor:

LESENNE Laurent, 26 rue des Tertres, F-35690 ACIGNE, FR, FR (Residence), FR (Nationality), (Designated only for: US)

PASQUIER Frederic, 26 rue d'Ouessant, F-35890 Laille, FR, FR (Residence), FR (Nationality), (Designated only for: US)

SCHAEFER Ralf, 5 rue du Martin Pêcheur, F-35690 ACIGNE, FR, FR (Residence), DE (Nationality), (Designated only for: US)

Legal Representative:

KERBER Thierry (agent), THOMSON multimedia, 46, quai Alphonse le Gallo, F-92648 Boulogne cedex, FR,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200296016 A2-A3 20021128 (WO 0296016)

Application: WO 2002EP5610 20020522 (PCT/WO EP0205610)

Priority Application: FR 20016769 20010523

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU

CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP

KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO

RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW

EP AT BE BG CH CY CZ DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

OA BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

AP GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW

EA, AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 13575

Fulltext Availability:

Detailed Description

Detailed Description

... K2 ... Kn of the enciphering library 15. The identification module 27 is designed to perform the identification according 1 5 to one of the identification **keys** Ki, as a **function** of instructions given by the **message** identification device 4. Moreover, the latter comprises an identification control unit 21, capable of triggering the identification module 27 by communicating the necessary information thereto...

...a unit 23 for extracting from the message MSG the key identifier KeyID, giving the current identification key Ki chosen in correspondence with the current **enciphering key** Ki of the sender 2.

The succinct account given above is essentially functional, and it is exclusively centred around specific features in conjunction with a particular assembly for securely protecting and identifying **messages**. The

sender 1 can in reality comprise several security devices such as that referenced 15, possibly in combination. For example, the secure protecting of the messages combines...

19/3,K/9 (Item 4 from file: 349)

DIALOG(R) File 349: PCT FULLTEXT

© 1994 WIPO/Univentio. All rts. reserv.

Image available

NON-TRANSFERABLE ANONYMOUS DIGITAL RECEIPTS RECUS NUMERIQUES ANONYMES NON TRANSMISSIBLES

Patent Applicant/Assignee:

INTERNATIONAL BUSINESS MACHINES CORPORATION, New Orchard Road, Armonk, NY 10504, US, US (Residence), US (Nationality), (For all designated states except: US)

Patent Applicant/Inventor:

CAMENISCH Jan, Bahnhofstrasse 13, CH-8803 Rueschlikon, CH, CH (Residence), CH (Nationality), (Designated only for: US)

VANHERREWEGHEN Elsie A, Sennhuettenstrasse 37, CH-8810 Horgen, CH, CH (Residence), BE (Nationality), (Designated only for: US)

Legal Representative:

WILLIAMS Julian David (agent), International Business Machines Corporation, Saeumerstrasse 4/Postfach, CH-8803 Rueschlikon, CH,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200287148 A1 20021031 (WO 0287148)

Application: WO 2002IB907 20020325 (PCT/WO IB0200907)

Priority Application: EP 2001810395 20010423

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU

CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP

KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO

RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 5328

Fulltext Availability:

Detailed Description

Detailed Description

... PA on at least the first value Pu and the second encryption E2 is the encryption of the second value Si, under the first public **key** Pu, the received second **encryption** E2 and ...ownership of the receipt Lu, that has been issued by the second party A, is verified.

The second validation packet B, indicated with box 4, **receives** a proof **message** PM from the user U, indicated with box 1. The proof **message** PM is **derived** from the first public **key** Pu that bases on the secret

19/3,K/10 (Item 5 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00926002 **Image available**

METHOD FOR TRACING TRAITOR RECEIVERS IN A BROADCAST ENCRYPTION SYSTEM
PROCEDE PERMETTANT DE REPERER DES RECEPTEURS ESPIONS DANS UN SYSTEME DE
CHIFFREMENT DE DIFFUSION

Patent Applicant/Assignee:

INTERNATIONAL BUSINESS MACHINES CORPORATION, New Orchard Road, Armonk,
New York, NY 10504, US, US (Residence), US (Nationality)
IBM UNITED KINGDOM LIMITED, P.O. Box 41, North Harbour, Portsmouth,
Hampshire PO6 3AU, GB, GB (Residence), GB (Nationality), (Designated
only for: MG)

Inventor(s):

WISNIECH Jeffrey Bruce, 982 Foothill Drive, San Jose, CA 95123, US,
MAOR Dalit, 247 Fulton Street, Palo Alto, CA 94301, US,
MAOR Simeon, 247 Fulton Street, Palo Alto, CA 94301, US,

Legal Representative:

BURT Roger James (agent), IBM United Kingdom Limited, Intellectual
Property Law, Hursley Park, Winchester, Hampshire SO21 2JN, GB,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200260118 A2-A3 20020801 (WO 0260118)
Application: WO 2002GB312 20020123 (PCT/WO GB0200312)
Priority Application: US 2001771239 20010126

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU

CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP

KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO

RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 8984

Fulltext Availability:

Detailed Description

Detailed Description

... receiver computes the subset key $L_{i,j}$ by evaluating the function G at most N times at block 68. Then, the receiver uses the subset **key** to **decrypt** the session **key** K at block 70 for subsequent message decryption.

Figure 13 shows how labels and, hence, subset keys, are assigned to receivers in the subset difference...

...off the direct path and that are induced by some node v_i , an ancestor of u. These labels establish the private information I_u of the **receiver** at block 74, with subsequent **message** session **keys** being encrypted with subset **keys** **derived** from the labels at block 76.

Referring briefly to Figure 14, the above principle is illustrated.

For every v_i ancestor with label S of a...

19/3,K/11 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

6000 **Image available**

METHOD FOR BROADCAST ENCRYPTION

PROCEDE DE CHIFFREMENT DE CONTENU DE DIFFUSION ET DE REVOCATION DE CLE DE
RECEPTEURS SANS ETAT

Patent Applicant/Assignee:

INTERNATIONAL BUSINESS MACHINES CORPORATION, New Orchard Road, Armonk, NY
10504, US, US (Residence), US (Nationality)

IBM UNITED KINGDOM LIMITED, PO Box 41, North Harbour, Portsmouth,
Hampshire PO6 3AU, GB, GB (Residence), GB (Nationality), (Designated
only for: MG)

Inventor(s):

LOTSPIECH Jeffrey Bruce, 982 Foothill Drive, San Jose, CA 95123, US,
NAOR Dalit, 247 Fulton Street, Palo Alto, CA 94301, US,
NAOR Simeon, 247 Fulton Street, Palo Alto, CA 94301, US,

Legal Representative:

BURT Roger James (agent), IBM United Kingdom Limited, Intellectual
Property Law, Hursley Park, Winchester, Hampshire SO21 2JN, GB,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200260116 A2-A3 20020801 (WO 0260116)

Application: WO 2002GB305 20020123 (PCT/WO GB0200305)

Priority Application: US 2001770877 20010126

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU

CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP

KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO

RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW

(AA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 10278

Fulltext Availability:

Detailed Description

Detailed Description

... receiver computes the subset key $L_{i,j}$ by evaluating the function G at
most N times at block

68. Then, the receiver uses the subset **key** to **decrypt** the session
key K

at block 70 for subsequent message decryption.

Figure 13 shows how labels and, hence, subset keys, are assigned to
receivers in the subset difference...

...off the direct path and that are induced by some node v_i , an ancestor of
 u . These labels establish the private information I_i of the **receiver** at
block 74, with subsequent **message** session **keys** being encrypted with
subset **keys** **derived** from the labels at block 76.

Referring briefly to Figure 14, the above principle

19/3,K/12 (Item 7 from file: 349)

File 349:PCT FULLTEXT

WIPO/Univention. All rts. reserv.

6000 **Image available**

TRUSTED INTERMEDIARY

INTERMEDIAIRE DE CONFIANCE

Patent Applicant/Assignee:

VLIQUITY CORPORATION, 1330 O'Brien Drive, Menlo Park, CA 94025, US, US
(Residence), US (Nationality)

Inventor(s):

JAIN Sandeep, 2312 Wooster Avenue, Belmont, CA 94002, US,

THAKUR Sudheer, 34, Nand Nagar Colony, ITI Road, 221005 Varanasi, IN,

JEU Kevin, 3475 Granada Avenue #327, Santa Clara, CA 95051, US,

Legal Representative:

HICKMAN Brian (et al) (agent), Hickman Palermo Truong & Becker, LLP, 1600
Willow Street, San Jose, CA 95125, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200254665 A1 20020711 (WO 0254665)
Application: WO 2002US81 20020104 (PCT/WO US0200081)
Priority Application: US 2001754907 20010104
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU
CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP
KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO
RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 8225

Fulltext Availability:
Detailed Description

Detailed Description

... in possession of the decryption key (private key) can decrypt the
message. Thus, the owner of a public key requests all parties that wish
to send the owner an encrypted- message, to encrypt the message
using the public key of the owner. All messages thus encrypted can only
be decrypted by the owner, using the owner's corresponding private key.

The public key technique...

...the other party's public key value to privately and securely compute a
private key, using an agreed-upon algorithm.
The parties then use their derived private keys in a separate
encryption algorithm to encrypt messages passed over the data
communication channel. Conventionally, these private keys are valid only
on a per communication session basis, and thus, are referred to as
session keys. These session keys...

19/3,K/13 (Item 8 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00920540 **Image available**

SECURITY BREACH MANAGEMENT
LUTTE CONTRE LES ATTEINTES A LA SECURITE

Patent Applicant/Assignee:

VIQUITY CORPORATION, 1330 O'Brien Drive, Menlo Park, CA 94025, US, US
(Residence), US (Nationality)

Inventor(s):

WAIN Sandeep, 2312 Wooster Avenue, Belmont, CA 94002, US,
THAKUR Sudheer, 34 Nand Nagar Colony, ITI Road, 221005 Varanasi, IN,
KEU Kevin, 3475 Granada Avenue #327, Santa Clara, CA 95051, US,
GHATARE Sanjay, 138 Sham Nagar, 444606 Amravati, IN,

Legal Representative:

HICKMAN Brian (et al) (agent), HICKMAN PALERMO TRUONG & BECKER, LLP, 1600
Willow Street, San Jose, CA 95125, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200254644 A1 20020711 (WO 0254644)
Application: WO 2002US82 20020104 (PCT/WO US0200082)
Priority Application: US 2001755851 20010105

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU
CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP
KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO
RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW

(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 7834

Fulltext Availability:
Detailed Description

Detailed Description

... in possession of the decryption key (private key) can decrypt the message. Thus, the owner of a public key requests all parties that wish to **send** the owner an encrypted **message**, to **encrypt** the message using the public **key** of the owner. All messages thus encrypted can only be decrypted by the owner, using the owner's corresponding private key.

The public key technique...

...the other party's public key value to privately and securely compute a private key, using an agreed-upon algorithm.

The parties then use their **derived** private **keys** in a separate encryption algorithm to encrypt **messages** passed over the data **communication** channel. Conventionally, these private keys are valid only on a per communication session basis, and thus, are referred to as session keys. These session keys...

19/3,K/14 (Item 9 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

Image available

SYSTEM AND METHOD OF BOOTSTRAPPING A TEMPORARY PUBLIC -KEY INFRASTRUCTURE
FROM A CELLULAR TELECOMMUNICATION AUTHENTICATION AND BILLING
INFRASTRUCTURE

SYSTEME ET PROCEDE D'INITIALISATION D'INFRASTRUCTURE D'UNE CLE PUBLIQUE
TEMPORAIRE A PARTIR D'UNE INFRASTRUCTURE D'AUTHENTIFICATION DE
TELECOMMUNICATION CELLULAIRE ET DE FACTURATION

Patent Applicant/Assignee:

NOKIA CORPORATION, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence),
FI (Nationality)

NOKIA INC, 6000 Connection Drive, Irving, TX 75039, US, US (Residence),
US (Nationality), (Designated only for: LC)

Inventor(s):

ASOKAN Nadarajah, Ankkurinvarsi 6 K, FIN-02320 Espoo, FI,
GINZBOORG Philip, Ylakaupinkuja 1 B 10, FIN-02360 Espoo, FI,

Legal Representative:

BRUNDIDGE Carl I (et al) (agent), Antonelli, Terry, Stout & Kraus, LLP,
Suite 1800, 1300 North Seventeenth Street, Arlington, VA 22209, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200221464 A2-A3 20020314 (WO 0221464)

Application: WO 2001IB1462 20010815 (PCT/WO IB01001462)

Priority Application: US 2000659781 20000911

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU

CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP

KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD

SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(EA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

(AF) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 11412

Fulltext Availability:
Claims

... mobile station 20 and used to identify this particular session. The gateway 60 in turn stores the SID and IMSI in its local memory and **transmits** the IMSI in **message** 220 to the HLRJAUC I 00 contained within home network operator service 80. The gateway 60 is able to identify which HLR /AUC 100...

...to FIG. 4, the HLRJAUC 100 responds with message 230 containing a random number (RAND) 410, a signed response (SRES) 450, and an **encryption key** (Kc) 400. The gateway 60 takes the Kc 400 and uses it to compute an integrity key (K) based on the formula $K = f(jKc)$...

...gateway 60 would then store the SID, IMSI, RAND 440, SRES 450 and K in a single record in the gateway--s 60 memory. Thereafter, **message** 240 is **sent** from the gateway 60 to the mobile station 20 and contains RAND 440 and M1. M1 is computed based upon a **message authentication code** (MAC) **function** using integrity **key** (K) and RAND 440. The formula used is represented as M1 MAC (K, JRANDI). The purpose of a MAC is to facilitate, without the...

19/3,K/15 (Item 10 from file: 349)
 DIALOG(R)File 349:PCT FULLTEXT
 (c) 2004 WIPO/Univentio. All rts. reserv.

Image available

METHOD AND APPARATUS FOR PROVIDING CONDITIONAL ACCESS IN CONNECTION-ORIENTED, INTERACTIVE NETWORKS WITH A MULTIPLICITY OF SERVICE PROVIDERS
 PROCEDE ET APPAREIL ASSURANT L'ACCES CONDITIONNEL A UNE MULTIPLICITE DE FOURNISSEURS DE SERVICES DANS DES RESEAUX INTERACTIFS DE TRANSMISSION EN MODE CONNEXION

Patent Applicant/Assignee:

SCIENTIFIC-ATLANTA INC,

Inventor(s):

WASILEWSKI Anthony John,

WOODHEAD Douglas F,

LOGSTON Gary Lee,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9724832 A1 19970710

Application: WO 96US13743 19960822 (PCT/WO US9613743)

Priority Application: US 95580759 19951229

Designated States: AU CA JP AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE

Publication Language: English

Fulltext Word Count: 16490

Fulltext Availability:

Claims

Claim

... 35, wherein the first keys are encrypted according to a Triple-DES algorithm.
 . A method as recited in claim 35, wherein the second keys are **encrypted** according to a public- **key** cryptographic technique.

39 A method as recited in claim 38, wherein the public-key cryptographic technique implements an RSA algorithm.

40 A method as recited...

...35, wherein the application of the message authentication code comprises the steps of concatenating the first key and the second key; and, hashing the concatenated **keys** in accordance with a

hashing function to produce said message authentication code .

41 A method as recited in claim 40, wherein the hashing function comprises a Message Digest 5 function.

42 A method as recited in claim 35, wherein step (i) further comprises the steps of:
(i) hashing a message that is comprised of the second key ;
(ii) encrypting the hash message with a public-key encryption algorithm using a private key associated with the SK, wherein the private key has a corresponding public key that is provided to the STU; and,
(iii) transmitting the encrypted hashed message to the authorized customer.

43 In a digital transmission system wherein groups of program bearing packets are transmitted over a digital network between a service...

19/3,K/16 (Item 11 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00323167 **Image available**

USER AUTHENTICATION IN A COMMUNICATIONS NETWORK
AUTHENTIFICATION DES UTILISATEURS DANS UN RESEAU DE COMMUNICATION

Patent Applicant/Assignee:

BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY,
HARDING Peter Maxwell,
HICKS Richard Middleton,
KINGAN Jonathan James,
MEYERSTEIN Michael Victor,
NOLDE Keith Eric,
RAESON John,
RANGER Jonathan Crispin,
ROBERTS David Anthony,
STIRLAND Mark Jonathan,
SWALE Richard Paul,

Inventor(s):

HARDING Peter Maxwell,
HICKS Richard Middleton,
KINGAN Jonathan James,
MEYERSTEIN Michael Victor,
NOLDE Keith Eric,
RAESON John,
RANGER Jonathan Crispin,
ROBERTS David Anthony,
STIRLAND Mark Jonathan,
SWALE Richard Paul,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9605675 A1 19960222
Application: WO 95GB1937 19950816 (PCT/WO GB9501937)
Priority Application: GB 9416595 19940817

Designated States: AM AT AU BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU
IS JP KE KG KP KR KZ LK LR LT LU LV MD MG MN MW MX NO NZ PL PT RO RU SD
SE SG SI SK TJ TM TT UA UG US UZ VN KE MW SD SZ UG AT BE CH DE DK ES FR
GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG

Publication Language: English

Text Word Count: 7597

Text Availability:
Detailed Description
Claims

Detailed Description

... key;

comparing the expected authentication code with the received authentication code; and
denying unrestricted access to the network for the terminal unless the expected and **received** authentication **codes** match.

The terminal may be part of an NTE with which the security node communicates to establish authentication or not. Alternatively, the terminal may be...

...key, the or each first key being loaded into the terminal for later use with the first algorithm in authenticating a terminal. Advantageously, the first **key** is a **function** of the terminal identification **code encrypted** by the second **key** using the security algorithm.

In a preferred embodiment, the transaction number is a variable number which is changed after each authentication attempt.

The security node...

...of the network.

Conveniently, the security node prevents access to the network for the terminal in the event that no match between the expected and **received** authentication **codes** is made within a predetermined duration.

Preferably, the terminal transmits a negative acknowledgement to the security node in the event that no challenge, or an...

claim

... an expected authentication code (E) at the security node based on the transaction number, the first algorithm and the first key; comparing the expected authentication **code** with the **received** authentication **code**; and
denying unrestricted access to the network for the terminal unless the expected and **received** authentication **codes** match.

2 A method as claimed in claim 1, in which the security node calculates at least one first key (Si) for the terminal, the...

...use with the first algorithm (F) in authenticating a terminal.

3 A method as claimed in claim 1 or claim 2, in which the first **key** is a
function of the terminal identification **code** (TN) **encrypted** by the second **key** (K) using the security algorithm (fi).

4 A method as claimed in any one of claims 1 to 3, in which the transaction number (n...also stored in the security node, and the first key, and to deny unrestricted access to the network for that terminal unless the expected and **received** authentication **codes** match. 1 5. A system as claimed in claim 14, in which the security node (10) includes means operable to calculate the first key (Sj...

...for later use in the authentication of that terminal.

6 A system as claimed in claim 14 or claim 15, in which the first **key** is a **function** of the terminal identification **code** (TN) **encrypted** by the second **key** (K) using the security algorithm (fi).

17 A system as claimed in any one of claims 14 to 16, in which the transaction number (n...

00228163

HIGH-SPEED MODULO EXPONENTIATOR DEVICE

DISPOSITIF RAPIDE D'ELEVATION A LA PUISSANCE MODULO

Patent Applicant/Assignee:

INTERNATIONAL STANDARD ELECTRIC CORPORATION,

Inventor(s):

CONFORTI Michael,

CLARK James Monroe,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9302413 A1 19930204

Application: WO 92US5990 19920717 (PCT/WO US9205990)

Priority Application: US 91228 19910722

Designated States: CA JP AT BE CH DE DK ES FR GB GR IT LU MC NL SE

Publication Language: English

Fulltext Word Count: 22214

Fulltext Availability:

Detailed Description

Detailed Description

... $47 \times 59 = 2773$, and $E = 17$, the

ciphertext $C = 92017 \pmod{2773} = 948$. Using $p = 47$ and

$q = 59$, a value $D = 157$ can be derived as the private **key** by

which the original **message** can be calculated as 948157

$\pmod{2773} = 920$, which is decoded as the word "IT".

Modular arithmetic plays a large part in public

key encryption systems because it uses smooth and continuous functions to obtain discontinuous values which jump around in a haphazard way. While the encryption method may be...

...code breaker's work

increases much more rapidly with increasing length N of the

numbers used than does the work of an authorized sender or

receiver. For example, if the **code** breaking work is

proportional to NN whereas the encrypting/decrypting work is

proportional to N^3 then doubling N from 10 to 20 makes an...

File 8: Ei Compendex(R) 1990-2004/Mar W1
(c) 2004 Elsevier Eng. Info. Inc.
File 35: Dissertation Abs Online 1861-2004/Feb
(c) 2004 ProQuest Info&Learning
File 12: Info. Sci. & Tech. Abs. 1966-2004/Feb 27
(c) 2004 EBSCO Publishing
File 65: Inside Conferences 1993-2004/Mar W2
(c) 2004 BLDSC all rts. reserv.
File 2: INSPEC 1969-2004/Mar W1
(c) 2004 Institution of Electrical Engineers
File 94: JICST-EPlus 1985-2004/Mar W1
(c) 2004 Japan Science and Tech Corp(JST)
File 6: NTIS 1964-2004/Mar W2
(c) 2004 NTIS, Intl Cpyrght All Rights Res
File 144: Pascal 1973-2004/Mar W1
(c) 2004 INIST/CNRS
File 434: SciSearch(R) Cited Ref Sci 1974-1989/Dec
(c) 1998 Inst for Sci Info
File 34: SciSearch(R) Cited Ref Sci 1990-2004/Mar W1
(c) 2004 Inst for Sci Info
File 99: Wilson Appl. Sci & Tech Abs 1983-2004/Feb
(c) 2004 The HW Wilson Co.
File 583: Gale Group Globalbase(TM) 1986-2002/Dec 13
(c) 2002 The Gale Group
File 266: FEDRIP 2004/Jan
Comp & dist by NTIS, Intl Copyright All Rights Res
File 95: TEME-Technology & Management 1989-2004/Feb W5
(c) 2004 FIZ TECHNIK
File 62: SPIN(R) 1975-2004/Jan W4
(c) 2004 American Institute of Physics
File 239: Mathsci 1940-2004/Apr
(c) 2004 American Mathematical Society

Item	Description
S1	1582313 MESSAGE? ? OR EMAIL OR MAIL OR TEXT OR CODE? ?
S2	11361 KEY? ?(5N) (DEPENDENT OR DEPENDENCE OR RELIAN?? OR CONTINGE- NT OR FUNCTION OR DERIV???)
S3	146834 S1(5N) (SEND??? OR SENT OR TRANSMIT? OR TRANSFER???? OR TRA- NSMISSION OR FORWARD??? OR RELAY??? OR CONVEY? OR DELIVER??? - OR COMMUNICAT? OR EXCHANG? OR BROADCAST??? OR DISTRIBUT??? OR RECEIV?)
S4	37335 CIPHER? OR CYPHER? OR ENCRYPT? OR ENCIPHER? OR ENCYPER? OR DECRYPT? OR DECIPHER? OR DECYPHER? OR UNENCIPHER? OR UNENCRY- PT? OR UNCIPHER?
S5	5792 SHARED(1W) (KEY OR DATA OR INFORMATION OR VALUE? ? OR NUMBE- R? ? OR CODE? ?)
S6	50151 KEY(3N) (ESTABLISH? OR GENERAT? OR CREAT???? OR FASHION? OR CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR PRODUC????? OR DEVELOP? OR BUILT OR BUILD?)
S7	22933 KEY(5N) (COMPUTE OR COMPUTES OR COMPUTED OR COMPUTING OR DE- TERMIN? OR DISCERN? OR DERIV? OR CALCULA?)
S8	195 S2(7N)S1
S9	7 S8 AND S3 AND S4
S10	6 RD (unique items)
S11	163 S6:S7(7N)MESSAGE
S12	31 S3 AND S4 AND S11
S13	16 RD (unique items)
S14	14 S13 NOT S10
	7 S14 NOT PY=1999:2004

10/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)
(c) 2004 Elsevier Eng. Info. Inc. All rts. reserv.

06718059 E.I. No: EIP04078018963

Title: E-Mail Security Gets Personal

Author: Paulson, Linda Dailey

Source: Computer v 37 n 1 January 2004. p 26

Publication Year: 2004

CODEN: CPTRB4 **ISSN:** 0018-9162

Language: English

Document Type: JA; (Journal Article) **Treatment:** T; (Theoretical)

Journal Announcement: 0402W3

Abstract: Voltage Security developed a simplified e-mail security system, called SecureMail that derives its public encryption key from a message sender's own e-mail address. SecureMail's server software uses one algorithm to convert an e-mail address into a number that functions as a public encryption key and another algorithm to create the user's private key based on the public one. The company states that its approach automates and simplifies the authentication process that establishes trust between two communicating parties. The system reduces complexity and potential management problems without a dedicated server to handle the secure transmissions. (Edited abstract)

Descriptors: *Security of data; Electronic mail; Public key cryptography; Servers; Computer software; Data communication systems; Encoding (symbols); Information management; User interfaces; Algorithms

Identifiers: Public key infrastructure technology; Authentication

Classification Codes:

723.2 (Data Processing); 723.5 (Computer Applications); 903.2 (Information Dissemination); 722.2 (Computer Peripheral Equipment)
723 (Computer Software, Data Handling & Applications); 722 (Computer Hardware); 716 (Electronic Equipment, Radar, Radio & Television); 903 (Information Science); 921 (Applied Mathematics)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATION ENGINEERING); 90 (ENGINEERING, GENERAL); 92 (ENGINEERING MATHEMATICS)

10/5/2 (Item 1 from file: 144)
DIALOG(R)File 144:Pascal
(c) 2004 INIST/CNRS. All rts. reserv.

1636515 PASCAL No.: 02-0023194

Chinese remainder theorem based hierarchical access control for secure group communication

Information and communications security : Xian, 13-16 November 2001

XUKAI ZOU; RAMAMURTHY Byrav; MAGLIVERAS Spyros S

SIHAN QING, ed; OKAMOTO Tatsuaki, ed; JIANYING ZHOU, ed

University of Nebraska-Lincoln, Lincoln NE 68588, United States; Florida Atlantic University, Boca Raton, Florida 33431, United States

ICICS 2001 : international conference on information and communications security, 3 (Xian CHN) 2001-11-13

Journal: Lecture notes in computer science, 2001, 2229 381-385

ISBN: 3-540-42880-1 **ISSN:** 0302-9743 **Availability:** INIST-16343; 354000097031590420

No. of Refs.: 11 ref.

Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)

Country of Publication: Germany; United States

Language: English

Secure group communication with hierarchical access control refers to a scenario where a group of members is divided into a number of subgroups located at different privilege levels and a high-level subgroup can receive and decrypt messages within any of its descendant lower-level subgroups; but the converse is not allowed. In this paper, we propose a new scheme CRTHACS, which is based on the Chinese Remainder Theorem. The scheme not only enables secure hierarchical control but also provides the following properties: hiding of hierarchy and receivers, authentication of both senders and messages, and a mechanism for the receiver to

directly derive the key of a message .

English Descriptors: Authentication; Hierarchized structure; China; Access control; Cryptography
Broad Descriptors: Asia; Asie; Asia

French Descriptors: Authentification; Structure hierarchisee; Chine; Controle acces; Cryptographie; Communication groupe securisee

Classification Codes: 001D04A04E

Copyright (c) 2002 INIST-CNRS. All rights reserved.

10/5/3 (Item 2 from file: 144)
DIALOG(R)File 144:Pascal
(c) 2004 INIST/CNRS. All rts. reserv.

14350716 PASCAL No.: 00-0001768
Periodical multi-secret threshold cryptosystems
Advances in cryptology - ASIACRYPT'99 : Singapore, 14-18 November 1999
NUMAO M
KWOK YAN LAM, ed; OKAMOTO Eiji, ed; CHAOPING XING, ed
Tokyo Research Laboratory, IBM, Ltd., 1623-14, Shimo-Tsuruma, Yamato, Kanagawa 242-8502, Japan
International conference on the theory and application of cryptology and information security (Singapore SGP) 1999-11-14
Journal: Lecture notes in computer science, 1999, 1716 363-377
ISBN: 3-540-66666-4 ISSN: 0302-9743 Availability: INIST-16343;
354000080104160290
No. of Refs.: 1 p.1/4
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: Germany
Language: English
A periodical multi-secret threshold cryptosystem enables a **sender** to **encrypt** a **message** by using a cyclical sequence of keys which are shared by n parties and periodically updated. The same keys appear in the same order in each cycle, and thus any subset of $t + 1$ parties can **decrypt** the message only in the periodical time-frames, while no subset of t corrupted parties can control the system (in particular, none can learn the **decryption** key). This scheme can be applied to a timed-release cryptosystem whose release time is determined when the number of share update phases equals the period of the sequence. The system is implemented by sharing a pseudo-random sequence generator function. It realizes $n \geq 3t + 1$ robustness, and is therefore secure against an adversary who can corrupt at most one third of the parties.

English Descriptors: Cryptography; **Message transmission** ; **Decryption** ; Control system; Implementation; Pseudorandom sequence; **Function** generation; **Encryption** ; Multisecret; Private **key**

French Descriptors: Cryptographie; **Transmission message** ; **Decryptage** ; Systeme commande; Implementation; Suite pseudoaleatoire; Generation fonction; Cryptage; Multisecret; Cle privee

Classification Codes: 001D04A04E

Copyright (c) 2000 INIST-CNRS. All rights reserved.

10/5/4 (Item 1 from file: 239)
DIALOG(R)File 239:Mathsci
(c) 2004 American Mathematical Society. All rts. reserv.

03301685 MR 2002h#94061
Almost $\$k\$$ -wise independent sample spaces and their cryptologic

applications.

Cryptography and coding (Cirencester, 1999)

Kurosawa, Kaoru (Department of Communications and Integrated Systems,
Tokyo Institute of Technology, Meguro, Tokyo, 152-8552, Japan)

Johansson, Thomas (Department of Information Technology, Lund University,
220 07 Lund, Sweden)

Stinson, Douglas R. (Department of Combinatorics and Optimization,
University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada)

Liu, Xian (Manchester School of Engineering, University of Manchester,
Manchester, M13 9PL, England)

Farrell, Patrick (Communications Research Centre, University of
Lancaster, Lancaster, LA1 4YR, England)

Boyd, Colin (School of Data Communications, Queensland University of
Technology, Brisbane, QLD 4001, Australia)

(Farrell, Patrick G.)

Corporate Source Codes: J-TOKYTE-IN; S-LUND-IFT; 3-WTRL-B; 4-MANC-SE;
4-LANC-CR; 5-QUT-SDC

1. Cryptology

Journal of Cryptology. The Journal of the International Association for
Cryptologic Research, 2001, 14, no. 4, 231--253. ISSN: 0933-2790

ACEN: JOCREQ

Springer, Berlin,; 84--93,,

Series: Lecture Notes in Comput. Sci., 1746,

Language: English Summary Language: English

Document Type: Journal

Journal Announcement: 200203

Subfile: MR (Mathematical Reviews) AMS; MR (Mathematical Reviews) AMS

Abstract Length: LONG (30 lines)

Summary: ``An almost k -wise independent sample space is a small subset
of m -bit sequences in which any k bits are 'almost independent'. We
show that this idea has close relationships with useful cryptological
notions such as multiple authentication codes (multiple A-codes), almost
strongly universal hash families, almost k -resilient functions, almost
correlation-immune functions, indistinguishable random variables and
 k -wise decorrelation bias of block **ciphers** .

``We use almost k -wise independent sample spaces to construct new
efficient multiple A- **codes** such that the number of **key** bits grows
linearly as a **function** of k (where k is the number of messages to be
authenticated with a single key). This improves on the construction of M.
Atici and D. R. Stinson [in Advances in cryptology---CRYPTO '96 (Santa
Barbara, CA), 15--30, Lecture Notes in Comput. Sci., 1109, Springer,
Berlin, 1996; MR 98g:94021], in which the number of key bits is
 $\Omega(k^2)$.

``We introduce the concepts of ϵ -almost k -resilient functions
and almost correlation-immune functions, and give a construction for almost
 k -resilient functions that has parameters superior to k -resilient
functions. We also point out the connection between almost k -wise
independent sample spaces and pseudorandom functions that can be
distinguished from truly random functions, by a distinguisher limited to
 k oracle queries, with only a small probability. Vaudenay has shown that
such functions can be used to construct block **ciphers** with a small
decorrelation bias.

``Finally, new bounds (necessary conditions) are derived for almost
 k -wise independent sample spaces, multiple A-codes and balanced
 ϵ -almost k -resilient functions.''

Reviewer: Summary Reviewer: Sgarro, Andrea (I-TRST)

Review Type: Signed review

Proceedings Reference: 2002d#94047; 1 861 825

Descriptors: *94A60 -Information and communication, circuits-
Communication, information-Cryptography (See also 11T71, 14G50, 68P25); *
94A60 -Information and communication, circuits-Communication, information-
Cryptography (See also 11T71, 14G50, 68P25) ; 94A62 -Information and
communication, circuits-Communication, information-Authentication and
secret sharing; 68P30 -Computer science (For papers involving machine
computations and programs in a specific mathematical area, see Section --04
in that area)-Theory of data-Coding and information theory (compression,
compression, models of communication, encoding schemes, etc.) (See also
94Axx); 94A40 -Information and communication, circuits-Communication,

information-Channel models, 94B40 -Information and communication ,
circuits-Theory of error-correcting codes and error-detecting codes-
Arithmetic codes (See also 11T71, 14G50)

10/5/5 (Item 2 from file: 239)

DIALOG(R)File 239:Mathsci

(c) 2004 American Mathematical Society. All rts. reserv.

02367627 MR 93d#94014

Combinatorial characterizations of authentication codes.

Johnson, L. R. (Department of Computer Science and Engineering,
University of Nebraska, Lincoln, Nebraska, 68588)

Corporate Source Codes: 1-NE-CS

Des. Codes Cryptogr.

Designs, Codes and Cryptography. An International Journal, 1992, 2,
no. 2, 175--187. ISSN: 0925-1022

Language: English

Document Type: Journal

Journal Announcement: 9214

Subfile: MR (Mathematical Reviews) AMS

Abstract Length: MEDIUM (17 lines)

Authentication coding involves a transmitter, a receiver and an opponent. The transmitter wants to communicate some source state s to the receiver, using a public communications channel. The source state is **encrypted** into a **message** which is **sent** through the channel. A key k defines the **message** $s(k)$ to be **sent** to communicate any s . Each **key** is a one-to-one **function** from the source space to the **message** space. A key source provides the transmitter with a key which, prior to any **message** being **sent**, is **communicated** to the receiver through a secure channel. In this paper, two combinatorial characterizations of authentication codes are given: authentication codes without secrecy (i.e., codes for which the message uniquely determines the source state, irrespective of the key being used) are characterized in terms of orthogonal arrays, and general authentication codes in terms of balanced incomplete block designs. In both cases, the keys must be equiprobable; in the second case, the source states must also be equiprobable.

Reviewer: Lobstein, Antoine (Paris)

Review Type: Signed review

Descriptors: *94A60 -Information and communication, circuits-
communication, information-Cryptography (See also 11T71, 68P25) ; 68P25 -
Computer science (For papers involving machine computations and programs in
a specific mathematical area, see Section --04 in that area)-Theory of data
-Data **encryption** (See also 94A60); 94B25 -Information and **communication**
, circuits-Theory of error-correcting **codes** -Combinatorial codes

10/5/6 (Item 3 from file: 239)

DIALOG(R)File 239:Mathsci

(c) 2004 American Mathematical Society. All rts. reserv.

01880464 MR 85k#68024

Proof checking the RSA public key encryption algorithm.

Boyer, Robert S. (Department of Computer Science, University of Texas,
Austin, 78712, Texas)

Moore, J. Strother (Department of Computer Science, University of Texas,
Austin, 78712, Texas)

Corporate Source Codes: 1-TX-C; 1-TX-C

Amer. Math. Monthly

The American Mathematical Monthly, 1984, 91, no. 3, 181--189.

ISSN: 0002-9890 CODEN: AMMYAE

Language: English

Document Type: Journal

Journal Announcement: 1609

Subfile: MR (Mathematical Reviews) AMS

Abstract Length: LONG (35 lines)

From the introduction: "Typical proofs in journal articles, textbooks,
and day-to-day mathematical communication use informal notation and leave

many of the steps to the reader's imagination. Nevertheless, by transcribing the sentences of the proof into a formal notation, it is sometimes possible to use today's automatic theorem-provers to fill in the gaps between published steps and thus mechanically check some published, informal proofs. In this paper we illustrate this idea by mechanically checking the recently published proof of the invertibility of the public key **encryption** algorithm described by R. L. Rivest, A. Shamir and L. Adleman [Comm. ACM 21 (1978), 120--126; Zbl 368:94005]. We briefly explain the idea of public key **encryption** to motivate the theorem proved. In the paper just cited a mathematical function, here called CRYPT, is defined. $\text{CRYPT}(M, e, n)$ is the **encryption** of message M with key (e, n) . The **function** has the following important properties: 1. It is easy to compute $\text{CRYPT}(M, e, n)$. 2. CRYPT is 'invertible', i.e., if M is **encrypted** with key (e, n) and then **decrypted** with key (d, n) , the result is M . That is, $\text{CRYPT}(\text{CRYPT}(M, e, n), d, n) = M$, under suitable conditions on M, n, e and d . 3. Publicly revealing CRYPT and (e, n) does not reveal an easy way to compute (d, n) . Public key **encryption** thus avoids the problem of distributing keys via secure means. Each user (e.g., a computer on a network) generates an **encryption** key and a corresponding **decryption** key, publicizes the **encryption** key, enables others to **send** private **messages**, and never **distributes** the **decryption** key.

15/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)
(c) 2004 Elsevier Eng. Info. Inc. All rts. reserv.

04549776 E.I. No: EIP96110408365

Title: **Multiple key distribution maintaining user anonymity via broadcast channels**

Author: Blundo, C.; Mattos, Luiz A. Frota; Stinson, D.R.
Corporate Source: Universita di Salerno, Baronissi, Italy
Source: Journal of Computer Security v 3 n 4 1994-1995. p 309-322
Publication Year: 1994-1995
EIN: 002468 ISSN: 0926-227X
Language: English
Document Type: JA; (Journal Article) Treatment: G; (General Review); T; (Theoretical)
Journal Announcement: 9701W1

Abstract: In this paper, we discuss methods by which a trusted authority can **broadcast** a **message** over a network, so that each member of a specified privileged subset of users can **decrypt** this **message** to **compute** a secret **key**. In contrast with previously constructed schemes, it is possible for the different privileged users to recover different keys from the **broadcast message**. Moreover, this is done in such a way that no coalition is able to recover any information on any of the keys they are not supposed to know. The schemes also do not require addressing, so user anonymity is maintained. The problem is studied using the tools of information theory, so the security provided is unconditional (i.e., not based on any computational assumption). Some useful schemes are presented and compared to previously known schemes. (Author abstract) 12 Refs.

Descriptors: *Security of data; Cryptography; Data communication systems; Information theory; Information retrieval; Data transfer

Identifiers: Multiple key distribution; User anonymity; Broadcast channels

Classification Codes:
723.2 (Data Processing); 716.1 (Information & Communication Theory);
903.3 (Information Retrieval & Use)
723 (Computer Software); 716 (Radar, Radio & TV Electronic Equipment);
71 (Information Science)
71 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATIONS); 90 (GENERAL ENGINEERING)

15/5/2 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2004 Institution of Electrical Engineers. All rts. reserv.

6031438 INSPEC Abstract Number: B9811-6120B-019, C9811-6130S-017

Title: **Some new results on key distribution patterns and broadcast encryption**

Author(s): Stinson, D.R.; Van Trung, T.
Author Affiliation: Dept. of Comput. Sci. & Eng., Nebraska Univ., Lincoln, NE, USA

Journal: Designs, Codes and Cryptography vol.14, no.3 p.261-79
Publisher: Kluwer Academic Publishers,
Publication Date: Sept. 1998 Country of Publication: Netherlands
ISSN: 0925-1022

SICI: 0925-1022(199809)14:3L.261:SRDP;1-G
Material Identity Number: 0660-98006
U.S. Copyright Clearance Center Code: 0925-1022/98/\$9.50
Language: English Document Type: Journal Paper (JP)
Treatment: Theoretical (T)

Abstract: This paper concerns methods by which a trusted authority can **distribute** keys and/or **broadcast** a **message** over a network, so that each member of a privileged subset of users can **compute** a specified **key** and **decrypt** the **broadcast message**. Moreover, this is done in such a way that no coalition is able to recover any information on a key or **broadcast message** they are not supposed to know. The problems are studied using the tools of information theory, so the security provided is unconditional (i.e., not based on any computational assumption). Stinson

(1997) described a method of constructing key predistribution schemes by combining Mitchell-Piper key distribution patterns with resilient functions, and also presented a construction method for broadcast encryption schemes that combines Fiat-Naor key predistribution schemes with ideal secret sharing schemes. We further pursue these two themes, providing several applications of these techniques by using combinatorial structures such as orthogonal arrays, perpendicular arrays, Steiner systems and universal hash families. (15 Refs)

Subfile: B C

Descriptors: combinatorial mathematics; cryptography; data privacy; information theory

Identifiers: key distribution patterns; broadcast encryption; trusted authority; broadcast message; information theory; unconditional security; Mitchell-Piper key distribution patterns; resilient functions; Fiat-Naor key predistribution; ideal secret sharing schemes; combinatorial structures; orthogonal arrays; perpendicular arrays; Steiner systems; universal hash families

Class Codes: B6120B (Codes); B0250 (Combinatorial mathematics); C6130S (Data security); C1160 (Combinatorial mathematics)

Copyright 1998, IEE

15/5/3 (Item 2 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2004 Institution of Electrical Engineers. All rts. reserv.

5771854 INSPEC Abstract Number: B9801-6120B-072, C9801-6130S-050

Title: On some methods for unconditionally secure key distribution and broadcast encryption

Author(s): Stinson, D.R.

Author Affiliation: Dept. of Comput. Sci. & Eng., Nebraska Univ., Lincoln, NE, USA

Journal: Designs, Codes and Cryptography vol.12, no.3 p.215-43

Publisher: Kluwer Academic Publishers,

Publication Date: Nov. 1997 Country of Publication: Netherlands

ISSN: 0925-1022

SICI: 0925-1022(199711)12:3L:215:SMUS;1-P

Material Identity Number: O660-97009

U.S. Copyright Clearance Center Code: 0925-1022/97/\$9.50

Language: English Document Type: Journal Paper (JP)

Treatment: Theoretical (T)

Abstract: This paper provides an exposition of methods by which a trusted authority can **distribute** keys and/or **broadcast** a **message** over a network, so that each member of a privileged subset of users can **compute** a specified **key** or **decrypt** the **broadcast message**. Moreover, this is done in such a way that no coalition is able to recover any information on a key or **broadcast message** they are not supposed to know. The problems are studied using the tools of information theory, so the security provided is unconditional (i.e., not based on any computational assumption). We begin by surveying some useful schemes for key distribution that have been presented in the literature, giving background and examples. In particular, we look more closely at the attractive concept of key distribution patterns, and present a new method for making these schemes more efficient through the use of resilient functions. Then we present a general approach to the construction of broadcast schemes that combines key predistribution schemes with secret sharing schemes. We discuss the Fiat-Naor broadcast scheme, as well as other, new schemes that can be constructed using this approach. (40 Refs)

Subfile: B C

Descriptors: cryptography; information theory

Identifiers: unconditionally secure key distribution; broadcast encryption; trusted authority; privileged subset; information theory; key distribution patterns; resilient functions; key predistribution schemes; secret sharing schemes; Fiat-Naor broadcast scheme

Class Codes: B6120B (Codes); B6110 (Information theory); C6130S (Data security); C1260 (Information theory)

Copyright 1997, IEE

15/5/4 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2004 Institution of Electrical Engineers. All rts. reserv.

04102512 INSPEC Abstract Number: B9204-6120B-040, C9204-6130S-059

Title: Non-interactive public-key cryptography

Author(s): Maurer, U.M.; Yacobi, Y.

Author Affiliation: Dept. of Comput. Sci., Princeton Univ., NJ, USA

Conference Title: Advances in Cryptology - EUROCRYPT '91. Workshop on the Theory and Application of Cryptographic Techniques Proceedings p.498-507

Editor(s): Davies, D.W.

Publisher: Springer-Verlag, Berlin, Germany

Publication Date: 1991 Country of Publication: West Germany xii+556

ISBN:

ISBN: 3 540 54620 0

Conference Sponsor: Int. Assoc. Cryptologic Res

Conference Date: 8-11 April 1991 Conference Location: Brighton, UK

Language: English Document Type: Conference Paper (PA)

Treatment: Theoretical (T)

Abstract: An identity-based non-interactive public key distribution system is presented that is based on a novel trapdoor one-way function allowing a trusted authority to compute the discrete logarithm of a given number modulo a publicly known composite number m while this is infeasible for an adversary not knowing the factorization of m . Without interaction with a key distribution center or with the recipient of a given message a user can generate a mutual secure **cipher** key based solely on the recipient's identity and his own secret key and **send** the **message**, **encrypted** with the **generated cipher key** using a conventional **cipher**, over an insecure channel to the recipient. Unlike in previously proposed identity-based systems, no public keys, certificates for public keys or other information need to be exchanged and thus the system is suitable for many applications such as electronic mail that do not allow for interaction. (28 Refs)

Subfile: B C

Descriptors: cryptography

Identifiers: identity-based non-interactive public key distribution system; trapdoor one-way function; trusted authority; discrete logarithm; mutual secure **cipher** key; electronic mail

Indexing Codes: B6120B (Codes); C6130S (Data security)

15/5/5 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2004 Institution of Electrical Engineers. All rts. reserv.

02824838 INSPEC Abstract Number: B87012927, C87011886

Title: Efficient microcomputer based exponentiation techniques for the RSA algorithm

Author(s): Crossfield, D.H.; Parish, D.J.

Author Affiliation: Plessey Network & Office Syst., Beeston, UK

Conference Title: Second International Conference on Secure Communication Systems (Conf. Publ. No.269) p.58-61

Publisher: IEE, London, UK

Publication Date: 1986 Country of Publication: UK 130 pp.

ISBN: 0 85296 339 4

Conference Sponsor: IEE

Conference Date: 27-28 Oct. 1986 Conference Location: London, UK

Language: English Document Type: Conference Paper (PA)

Treatment: Theoretical (T)

Abstract: Describes an efficient practicable solution for the production of two prime numbers (P,Q) needed for the generation of the public key (E). From P and Q the Euler function can be calculated and with a suitable algorithm the private key (D) can be **discerned**. **Encryption** involves the **message** being raised to the power of $E \bmod N$ ($N=P.Q$) and **decryption** involves raising the **transmitted message** to the power of $D \bmod N$. Both processes require the methods established. Work is continuing on this investigation to transfer the high level implementation to a low

level assembly language operating on a small 32 bit microcomputer. It is hoped that the results will indicate that it is feasible to produce a stand alone board for use as data security on local area networks. (2 Refs)

Subfile: B C

Descriptors: cryptography; microcomputer applications

Identifiers: **encryption**; microcomputer based exponentiation; RSA

Algorithms: prime numbers; public key; private key; **decryption**

Class Codes: B6120B (Codes); C6130 (Data handling techniques)

15/5/6 (Item 1 from file: 266)

DIALOG(R)File 266:FEDRIP

Comp & dist by NTIS, Intl Copyright All Rights Res. All rts. reserv.

00188327

IDENTIFYING NO.: 0310297 AGENCY CODE: NSF

Practical Yet Provably Secure Public-Key Primitives

PRINCIPAL INVESTIGATOR: Shoup, Victor

PERFORMING ORG.: New York University, Computer Science, New York, NY

10012

PROJECT MONITOR: Landwehr, Carl E.

SPONSORING ORG.: National Science Foundation, CCR, 4201 Wilson Boulevard, Arlington, Virginia 22230

DATES: 20030815 TO 20050731 FY : 2003 FUNDS: \$700,000 (700000)

SUMMARY: NSF Proposal 0310297 Practical yet Provably Secure Public-Key Primitives Victor Shoup This research addresses the fundamental building blocks, or primitives, of public-key cryptography, and attempts to design and analyze new primitives that improve the state of the art, either through increased efficiency or increased security. The objectives are to design new primitives suitable for publication in academic journals, as well as for submission to relevant standards bodies. The methods used include (1) the "reductionist" approach of modern cryptography, whereby the security of a scheme is formally reduced to the presumed intractability of well-studied mathematical problems (e.g., factoring), and (2) algorithmic techniques from number theory and algebra. Public-key cryptography plays an essential role in securing computers and communication networks. The two basic public-key primitives are public-key **encryption** and digital signatures. The first primitive allows a **sender** to secretly **transmit** a **message** to a **receiver**, where the **sender** only needs to know a public key (known to everyone), while only the receiver needs to know the corresponding secret key. The second primitive allows a signer, using a secret **key**, to **generate** a digital signature on a **message** so that the signature can later be verified by any party using a corresponding public key. Although substantial progress has been made in recent years on these problems, there is still more work to do, in terms of improving the efficiency of the schemes, reducing the strength of the intractability assumptions, improving the quality of the security reductions, and in developing practical distributed versions of these schemes so as to avoid a single point of failure. These are the specific tasks taken on by this research.

15/5/7 (Item 1 from file: 239)

DIALOG(R)File 239:Mathsci

(c) 2004 American Mathematical Society. All rts. reserv.

01629368 MR 81g#94042

Bounds on message equivocation for simple substitution ciphers .

Dunham, James G.

IEEE Trans. Inform. Theory

Institute of Electrical and Electronics Engineers. Transactions on Information Theory, 1980, 26, no. 5, 522--527. ISSN: 0018-9448

CODEN: IETTAW

Language: English

Document Type: Journal

Journal Announcement: 1226

Subfile: MR (Mathematical Reviews) AMS

Abstract Length: SHORT (9 lines)

Author's summary: "For simple substitution ciphers an exact expression and bounds are derived for the message equivocation in terms of the key equivocation. It is established that the message equivocation approaches the key equivocation exponentially fast for discrete memoryless sources. It is observed that the exponential behavior of the message equivocation is not determined by redundancy in the message source but by either the symbol probabilities which are closest in a certain sense or the sum of the two smallest symbol probabilities."